NAVAL
POSTGRADUATE
SCHOOL

THESIS

RISK ASSESSMENT OF THE NAVAL POSTGRADUATE SCHOOL GIGABIT NETWORK

by

Dennis Rowlands
and
Todd Shumaker

September 2004

Thesis Co-Advisors: Karen Burke
Craig Rasmussen

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Risk Assessment of the Naval Postgraduate School Gigabit Network	**5. FUNDING NUMBERS**
6. AUTHOR(S) Dennis Rowlands and Todd Shumaker	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This research thoroughly examines the current Naval Postgraduate School Gigabit Network security posture, identifies any possible threats or vulnerabilities, and recommends any appropriate safeguards that may be necessary to counter the found threats and vulnerabilities. The research includes any portion of computer security, physical security, personnel security, and communication security that may be applicable to the overall security of both the .mil and .edu domains. The goal of the research was to ensure that the campus network is operating with the proper amount of security safeguards to protect the confidentiality, integrity, availability, and authenticity adequately from both insider and outsider threats. Risk analysis was performed by assessing all of the possible threat and vulnerability combinations to determine the likelihood of exploitation and the potential impact the exploitation could have on the system, the information, and the mission of the Naval Postgraduate School. The results of the risk assessment performed on the network are to be used by the Designated Approving Authority of the Naval Postgraduate School Gigabit network when deciding whether to accredit the system.

14. SUBJECT TERMS DITSCAP, Certification, Accreditation, Information Assurance, SSAA, Risk Assessment, Threat, Vulnerability, Risk, Countermeasure	**15. NUMBER OF PAGES** 149
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

RISK ASSESSMENT OF THE NAVAL POSTGRADUATE SCHOOL GIGABIT NETWORK

Todd Shumaker
Civilian, Research Associate
B.S., California State University, Bakersfield, 2003

Denny Rowlands
Civilian, Research Associate
B.S., Indiana University of Pennsylvania, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Authors: Denny Rowlands

Todd Shumaker

Approved by: Karen Burke
Thesis Co-Advisor

Craig Rasmussen
Thesis Co-Advisor

Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research thoroughly examines the current Naval Postgraduate School Gigabit Network security posture, identifies any possible threats or vulnerabilities, and recommends any appropriate safeguards that may be necessary to counter the found threats and vulnerabilities. The research includes any portion of computer security, physical security, personnel security, and communication security that may be applicable to the overall security of both the .mil and .edu domains. The goal of the research was to ensure that the campus network is operating with the proper amount of security safeguards to protect the confidentiality, integrity, availability, and authenticity adequately from both insider and outsider threats. Risk analysis was performed by assessing all of the possible threat and vulnerability combinations to determine the likelihood of exploitation and the potential impact the exploitation could have on the system, the information, and the mission of the Naval Postgraduate School. The results of the risk assessment performed on the network are to be used by the Designated Approving Authority of the Naval Postgraduate School Gigabit network when deciding whether to accredit the system.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Todd and Denny would like to thank their co-advisors, Karen Burke and Craig Rasmussen for their helpful insight throughout the entire thesis process. They would also like to thank Terri Brutzman and Lonna Sherwin for putting up with their endless questions about the Naval Postgraduate School's network and answering them as best they could. Without them, this thesis would not have been possible. This material is based upon work supported by the National Science Foundation under Grant No. 0114018. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. HISTORICAL BACKGROUND

1. The DITSCAP

Within the past ten years, the Department of Defense (DoD) has taken significant steps to ensure the confidentiality, integrity, and availability of information located in their own computer systems by implementing a procedure known as certification and accreditation. In December of 1997, the DoD released Instruction 5200.40 titled "DoD Information Technology Security Certification and Accreditation Process". This Instruction, known as the DITSCAP, mandates that any DoD system that collects, stores, transmits, or processes unclassified or classified information must undergo the certification and accreditation process. The necessity to perform certification and accreditation on all systems was reinforced when the DoD released the new Information Assurance policy in October of 2002. DoDD 8500.1, which supersedes the prior DoDD 5200.28, requires that all DoD systems be certified and accredited in accordance with DoD Instruction 5200.40.

The terms *certification* and *accreditation* are used to describe the two-tiered process implemented by the DoD to assure that all of their computer systems are operating at an acceptable level of risk. The National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009 defines the two terms as follows:

> Certification is the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.
>
> Accreditation is the formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [Ref. 1]

In most cases, certification is performed by a Certification Authority (CA) which assigns either a Certification Agent, or with larger systems, a team of Certification Agents to evaluate the level of compliance the system has with the predefined security requirements. It is the job of the CA to provide the Designated Approving Authority (DAA) with enough evidence to make an accreditation decision. The DAA is the official with the responsibility of formally approving or disapproving a system to become operational based on the ability of the system to meet certain security specifications. The DAA employs both the Information System Security Manger (ISSM) as principal advisor in Information Assurance matters and the Information System Security Officer (ISSO) to ensure security of the system from design to destruction. Other key members in the certification and accreditation process are the User Representative and the Program Manager (PM). The User Representative can be either a single person or an organization that speaks for the users of the system concerning the relationship/impact of security requirements on the operational mission. The PM is responsible for ensuring the security design and the overall development of the system. The Certification Agent, CA, DAA, User Representative, ISSM, and ISSO support the PM in all security related issues that may occur during the life-cycle of the system.

The DITSCAP is a four-phase process that is intended to address security issues during every step of the computer system life cycle. The first phase, known as the Definition phase, is focused on determining the mission, environment, and architecture of the system to identify the level of effort required for accreditation. The level of effort is a measurement that weighs seven system characteristics to determine both the density of security safeguards needed to protect the system adequately and the amount of resources required to provide the DAA with a sufficient amount of information about the system to make an accreditation decision. The end result of the Definition Phase is a System Security Authorization Agreement (SSAA) that outlines both the approach for the certification and accreditation effort and the security features necessary for the system at the predefined level of effort. The SSAA is then signed by the DAA, the PM, the Certification Agent, and the User Representative, and represents a formal agreement between the four parties.

The second phase of the DITSCAP is the Verification phase. This phase is implemented to provide further detail on the security requirements and their implementation, to revise and expand the SSAA when changes to security strategies are made, and to ensure compliance between the system being developed and the requirements agreed upon in the SSAA. Ensuring compliance is a lengthy task that could involve analysis of the system architecture, software design, network design, integrated products such as COTS or GOTS, system vulnerabilities, and life-cycle management. The goal of the Verification phase is to make certain before moving on to the next phase that the design and development efforts have yielded a system that will prove through testing to be both certifiable and accreditable.

The Validation phase of the DITSCAP includes the continuing evolution of the SSAA to reflect the status of the current system, certification evaluation and validation of the fully integrated system with the current security specifications in the SSAA, a possible system certification from the Certification Agent based on the compliance of the fully integrated system to the SSAA, and finally an accreditation decision by the DAA that could result in an authorization to operate for the system in question. The intensity and quantity of certification evaluation tasks performed in the Validation phase depends in large part on the level of effort measure assigned to the certification and accreditation process during the Definition phase. Certification evaluation may include system security testing, penetration testing, TEMPEST testing, COMSEC compliance validation, system management analysis, contingency plan evaluation, and a risk-based management review.

If after performing these evaluation tasks the Certification Agent is satisfied that the system complies with the agreed-upon security requirements, the agent will certify the system and recommend accreditation to the DAA. If the DAA decides to accredit the system, a detailed description of the operating environment and security parameters under which the system has been granted an authorization to operate will be provided in the accreditation documentation. Conversely, if the agent denies certification, the system is not accredited, and the certification and accreditation process is restarted again at the Definition phase. If a system is deemed to be mission critical and is required to be operational, an interim authorization to operate may be granted while additional security safeguards are implemented. In this scenario, it is also necessary for the system to return to the Definition phase to agree upon new security solutions and a schedule for completion.

The Post-Accreditation phase of the DITSCAP begins after the system has been accredited by the DAA and fully integrated into the predefined operating environment. This phase consists of multiple activities that are performed to maximize the probability that the accredited system will continue to operate with an acceptable level of risk. These activities include an ongoing effort to keep the SSAA current, evaluation of the system operations, change management, and compliance validation. The evaluation of system operations is performed periodically by the Information System Security Officer to ensure that the system is operating within the parameters detailed during accreditation. Any significant changes to the operating environment that may affect the security posture of the system must be agreed upon by the four parties that signed the SSAA. All systems that remain operational must be recertified and reaccredited after any major change to the security posture of the system occurs or following a set time frame that differs from one DoD department to the next. The circumstances that trigger recertification and reaccreditation must be detailed in the SSAA of the system.

2. Risk Management

A phrase that prominently appears in every phase of the DITSCAP is acceptable level of risk. It is generally acknowledged and accepted that every system operates with multiple risks at any given time because monetary constraints and the nature of software make it impossible to eliminate all risk. The NSTISSI 4009 defines risk as follows:

> A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact. [Ref. 1]

The amount of risk that is regarded as acceptable varies from system to system based on many factors including mission criticality, the classification level of information, and the potential impact the execution of the risk could inflict on the organization. Ultimately, it is the responsibility of the DAA to decide whether the level of risk is acceptable after reviewing the risk management results documented by the Certification Agent.

Risk management is a constant process and an inexact science that seeks a balance between the cost to protect an information system and the value of the assets to be protected. The job of risk management is to identify risks, assess them for their potential impact, and implement security safeguards that are economically feasible for the assets being protected. Risk management is a two phase process that consists of risk assessment and risk mitigation. Risk assessment is the first phase of risk management and consists of all the procedures responsible for identifying risks and their potential impact. Risk mitigation then utilizes the results found during risk assessment to apply controls and minimize risk wherever possible. These two processes are performed many times throughout the development of a system and combine to make risk management an essential procedure for establishing an acceptable level of risk within the DITSCAP.

Risk management is an iterative process that is performed by the Certification Agent at every stage of the system life-cycle, and consequently, every phase of the DITSCAP. During the Definition phase, a conceptual assessment is done to examine the security of the system design. A preliminary assessment is completed during the Verification phase to evaluate the security of the system during development and integration. A residual assessment is performed during the Validation phase to determine which risks remain after the countermeasures have been applied following the previous phases and before integration. After the system has been accredited, periodic compliance reviews are performed to ensure that the security of the system in the present operating environment maintains an acceptable level of risk. The results obtained from early life-cycle stages are used by subsequent stages for risk mitigation and risk is gradually decreased as a cumulative effect through the development of the system. When risk management is performed after the system is fully integrated into the operating environment during the Validation phase, the results are used by the DAA in the accreditation decision.

3. DoN Implementation

The Department of the Navy (DoN) developed the Naval Information Assurance Publication (IA Pub) 5239 series to provide guidance, procedures, and processes for implementing the DoN Information Assurance Program. Several modules in this series were written specifically to address information security (INFOSEC) issues. Because the DoD encompasses all branches of the military, the DoN is required to apply the DITSCAP to all Navy information systems. IA Pub 5239-13 is a three-volume module that pertains exclusively to the certification and accreditation process. Volume one introduces and summarizes the certification and accreditation process that is detailed in the DITSCAP and briefly describes the contents and uses for Volume two and Volume three. Volume two describes the certification and accreditation process that the DoN prescribes for systems that require only a basic level of information assurance. IA Pub 5239-01 defines five levels of information systems based on mission criticality and function. Of these five levels, Administrative and Mission Support systems generally only require completion of the certification and accreditation checklist provided in Volume two to satisfy the demands of the DITSCAP. Volume three details the certification and accreditation process designated for systems that necessitate more stringent levels of information assurance. This process applies to information systems defined by IA Pub 5239-01 to be either Mission Critical Category 1, 2, or 3.

IA Pub 5239-16 is the DoN Risk Assessment Guidebook that was developed to provide a standardized approach to assessing the level of risk in DoN information systems. This module of the 5239 series is intended for Certification Agents preparing the risk analysis appendix of the SSAA used by the DAA in the accreditation decision. If possible, the procedures in this module are to be used during every stage of the system life-cycle. However, for obvious reasons, it is possible that a Certification Agent will be unable to complete risk assessment during the design and development stages when certifying an operational system. The system administration guide should include the appropriate procedures for configuring the system to meet the criteria in the checklist. IA Pub 5239-16 implements a six-step process that consists of System Characterization, Threat Identification, Vulnerability Identification, Risk Analysis, Countermeasure Recommendations, and Assessment Results Documentation.

System Characterization defines the scope of the risk assessment effort by thoroughly identifying and documenting all technical and non-technical elements located inside the boundary of the information system. The documented results from System Characterization are used for analysis in every other step of the DoN risk assessment process. In some cases, the Certification Agent will find much of the needed information already assembled in the SSAA of the system. IA Pub 5239-16 suggests that at minimum the following information be collected:

- Hardware Components
- Software
- Internal and external system interfaces
- Data and information stored, processed, transferred, and used in the system
- Support personnel
- Users and their organizations
- The mission of the system
- The business processes the system performs
- The value or importance of the system and its data to the organization
- The classification and sensitivity of the system
- Documentation of system requirements
- Governing security policies
- System diagrams and flow charts
- Descriptions of the physical and environment security measures that will be in place

The Threat Identification and Vulnerability Identification steps are performed in parallel and the results from these two steps are used as input for Risk Analysis. During Threat Identification, the Certification Agent is responsible for identifying any potential situation that may disrupt the system, and consequently, impair the mission or personnel that the system supports. The NSTISSI 4009 defines a threat as follows:

> Any circumstance or event with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of the data, and/or denial of service. [Ref. 1]

The Certification Agent must document any potential natural, human, or environmental threat and approximate the likelihood of that occurrence happening and having an adverse affect on the system with the current amount of security safeguards. The Certification Agent must also estimate the motivation, resources, and capabilities necessary to execute a successful attack for each of the possible human threats. The IA Pub 5239-16 lists the following as examples of potential threat-agents:

- Floods, earthquakes, landslides, or hurricanes
- Human errors, including mistakes made while entering data into a system
- Human negligence
- Deliberate attempts to circumvent or damage a system and/or the security countermeasures designed to protect it
- Malicious code, such as viruses and Trojan horses
- Attempts to access information without proper authorization
- Long-term power failures
- Failure of building infrastructure components, such as burst water pipes or leaking roofs

During Vulnerability Identification, the Certification Agent must identify all potential flaws in the system. The NSTISSI 4009 defines a vulnerability as follows:

> Any weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. [Ref. 1]

The Certification Agent may take advantage of several valuable resources when searching for system vulnerabilities including government and vendor security advisories, previous risk assessment documentation, and system usage and audit reports. The Information Assurance Vulnerability Management (IAVM) process was developed by the Defense Information Systems Agency (DISA) in an effort to track all intentional or unintentional attempts to exploit DoD systems and they provide the Certification Agent with a powerful database consisting of known system flaws. The search for vulnerabilities is not limited to hardware and software flaws and may include weaknesses in procedures, policy, and configuration.

Risk Analysis is the longest and most demanding portion of the risk assessment process and relies heavily upon the results generated from System Characterization, Threat Identification, and Vulnerability Identification. The Certification Agent must determine the probability of exploitation for every possible threat and vulnerability combination and examine the potential impact the exploitation would have on the system, the information, the mission, and national security. IA Pub 5239-16 lists the four key factors for obtaining this information as criticality of the system and its data, the likelihood of successful exploitation, the magnitude of the impact of an attack, and the assigned level of risk.

Criticality of the system and its data is a rating that is used to measure the significance the system and information have to the mission, users, and organization. The rating is obtained by assessing the affect a compromise to the confidentiality, integrity, and availability of the system would have on the overall mission. A high rating denotes a system that is absolutely essential to all or part of the mission and may imply the presence of information that could cause dire consequences if compromised by an enemy. A medium rating represents a system that is very important to an organization, but the mission could be completed with the implementation of expensive contingency plans following a system compromise. A low rating signifies a system that would cause minimal burden to the mission in the event of system loss or degradation. A high criticality rating generally corresponds to an adversary having increased motivation to attack the system. Therefore, the criticality rating is an important factor in deciding the amount of security safeguards an information system requires.

The second factor involved in accomplishing the goals of the Risk Analysis step is assessing and rating the likelihood of successful exploitation. The Certification Agent examines each threat and vulnerability combination to determine how likely the scenario is to occur. A success probability is established by evaluating the relationship between the availability of resources required to exploit a vulnerability, a threat-agent's motivation to exploit that vulnerability, and the planned or existing technical and non-technical countermeasures intended to repel an attack. A high rating represents a scenario that requires a minimal level of effort by the attacker or a motivated and capable adversary with the means to exploit a vulnerability. A medium rating represents a situation that requires moderate effort and an attacker with considerable resources and motivation. A low rating signifies a system that has the proper safeguards implemented to defend an attacker or the adversary lacks the resources or motivation to exploit the vulnerability.

Magnitude of the impact of an attack is a rating used to determine the affect a successful exploit of a vulnerability may have on the mission. The impact is based on the loss of confidentiality, integrity, availability, and accountability of the system and information. Confidentiality is defined as the assurance that information is not disclosed to unauthorized persons, processes, or devices. Integrity is the assurance that information is consistent and has not been altered intentionally or unintentionally by someone or something without proper privileges. Availability is the assurance that the system and the data can be accessed by authorized users in an acceptable amount of time. Accountability provides assurance that all activities occurring on a system can be traced unquestionably to a source or a user. A high rating represents an attack that significantly impacts the system and could result in serious injury or death to the users of the system. A medium rating signifies an attack that could temporarily have a serious impact on the system. A low rating represents an attack that is easily detected and corrected without any lasting or negative affect on the system. A magnitude rating should be given to each threat and vulnerability combination.

The Certification Agent uses the previous three factors in determining the assigned level of risk for each threat and vulnerability combination. The results of these combinations are compared against a two-dimensional matrix that is constructed with the likelihood of exploitation ratings as the columns and the magnitude of impact ratings for the rows. Cells in the matrix that represent a high likelihood and a high magnitude combination are labeled with a high assigned level of risk. As the risk of exploitation and magnitude decrease, so to does the assigned level of risk rating. The Certification Agent initially assigns each threat and vulnerability combination an assigned level of risk based on the matrix and refines the rating based on factors such as past experience, criticality rating, and data classification.

In the next step of the risk assessment process, the Certification Agent is responsible for recommending necessary countermeasures to lower risk to a level acceptable for accreditation. The Certification Agent must work with the PM to implement the appropriate safeguards. Cost benefit analysis should be performed for every recommended countermeasure to weigh the cost of the safeguard against the expected improvement to the system. IA Pub 5239-16 lists the following as possible areas for security controls:

- Organizational policy and procedures
- Operational management
- Technical countermeasures
- Procedural
- Any other additional tools

The final step of the risk assessment process is developing the Assessment Results Documentation that is included as an appendix of the system SSAA and reviewed by the DAA during the accreditation decision. This documentation should be as thorough as possible because it will be referenced often in the continuing effort to manage the level of risk. The documentation will include the risk assessment approach, a threat statement, a detailed description and the recommended countermeasures for each finding, and the statement of risk. The statement of risk is the last section of the report and describes the overall level of risk in the system. This statement is prepared by the Certification Agent by evaluating the current vulnerabilities and countermeasures present in the system and assigning an aggregate level of risk.

B. PURPOSE OF STUDY

1. Scope

The Naval Postgraduate School is a part of both the Department of Defense and the Department of the Navy. Because of these affiliations, the Naval Postgraduate School and its computer systems must strictly adhere to the technical security policies implemented by both organizations. In particular, DoDD 8500.1 mandates that all computer systems operated by the Naval Postgraduate School must complete the procedures and processes of DoDI 5200.40, otherwise know as certification and accreditation. Further, the certification and accreditation process in regards to the Naval

Postgraduate School and its systems must follow the guidelines outlined in the DoN IA Pub 5239 series. More precisely, the three-volume 5239-13 module deals specifically with the requirements detailed in DoDI 5200.40.

Both the DoDI 5200.40 and the DoN IA Pub 5239-13 require risk analysis to be performed during all four phases of certification and accreditation and every life cycle stage of a system. DoN IA Pub 5239-16 was explicitly developed to assist the certification team in performing a risk assessment on a DoN System. The Naval Postgraduate School campus network is currently undergoing the certification and accreditation process and therefore must also be thoroughly examined for all existing and potential risk before being certified and accredited. This thesis will examine the current security posture of the Naval Postgraduate School network by performing each of the six steps included in the DoN IA Pub 5239-16 guide to risk assessment. The six steps included in the DoN risk assessment process are as follows:

- System Characterization
- Threat Identification
- Vulnerability Identification
- Risk Analysis
- Countermeasure Recommendations
- Assessment Results Documentation

This research will thoroughly examine the current Naval Postgraduate School Gigabit Network security posture, identify any possible threats or vulnerabilities, and recommend any appropriate safeguards that may be necessary to counter the found threats and vulnerabilities. The research will include any portion of computer security, physical security, personnel security, and communication security that may be applicable to the overall security of the campus network. The goal is to ensure that the campus network is operating with the proper amount of security safeguards to protect the confidentiality, integrity, availability, and authenticity from both insider and outsider threats. Risk analysis will be performed by assessing all of the possible threats vulnerabilities to determine the likelihood of exploitation and the potential impact the exploitation could have on the system, the information, and the mission of the Naval

Postgraduate School. The results of the risk assessment performed on the network may be used by the Designated Approving Authority of the Naval Postgraduate School Gigabit network when deciding whether to accredit the system.

2. Research Questions

In an effort to identify all of the current and potential risks associated with the Naval Postgraduate School Campus network, this paper will attempt to answer the following questions:

- Why must the NPS campus network undergo such a rigorous risk assessment process?
- How is the NPS campus network currently set up and configured?
- What is the DoD Level of Effort requirement for the network?
- What is the DoD Mission Assurance Category for the network?
- How does the current network configuration relate to the overall security?
- What is the current security posture of the NPS campus network?
- What are the current vulnerabilities of the network?
- What are the current threats to the network?
    - What are the inside threats?
    - What are the outside threats?
- What are the most likely vulnerabilities and threats for an attacker to potentially exploit?
- What impact would the exploitation of these vulnerabilities and threats have on the system, information, and mission?
- What safeguards and countermeasures can be implemented to reduce the risk of these vulnerabilities and threats from being exploited?
- Does the network meet the minimum security requirements for operation at the pre-determined Level of Effort and Mission Assurance Category?
- Should the Designated Approving Authority accredit the system?

3. Research Objectives

The overall objective of this research is to provide the key participants of the certification and accreditation process with information that will help them to determine the resources needed to protect the system adequately, to implement countermeasures required to secure the NPS campus network properly, and to reach an accreditation decision. The ISSM will be able to implement the countermeasure recommendations to strengthen the security of the network. The Certification Agent will be able to focus on the areas of the system that may require some extra attention. Finally, the DAA will be able to combine the information provided by this report, the complete security details located in the SSAA, and the advice given by the Certification Agent to make an educated accreditation decision. The goal is to ensure that the NPS campus network is equipped with enough security safeguards to protect the system from all inside and outside threats and to maintain the impeccable reputation of the Department of Defense and Department of the Navy.

C. ORGANIZATION OF PAPER

This paper will be organized much like the recommended output of IA Pub 5239-16. However, there have been some minor changes made in the outline of the report in an effort to clarify the most important findings of the risk assessment. The Vulnerability Identification and the Risk Analysis chapters have been combined to increase the effectiveness of the results and to facilitate the implementation of the countermeasures. Also, because this report will not actually be attached as an appendix to the official SSAA, the Assessment Results Documentation will be presented in a less formal manner and will be located in the Countermeasure and Conclusion chapters. First, the network and the security posture will be thoroughly examined during the System Characterization chapter. Second, the threats facing the NPS campus network will be detailed in the Threat Identification chapter. Next, the vulnerabilities will be presented with a risk analysis that will examine the likelihood, magnitude, and overall risk each of the vulnerabilities may have on the mission of the Naval Postgraduate School. Finally, the recommended countermeasures to strengthen the security of the network will be given. The complete outline of the paper is as follows:

- Introduction
    - Historical Background
    - Purpose of Study
        - Scope
        - Research Questions
        - Research Objectives

    - Organization of Paper
- System Characterization
    - Identify resources and information that constitute the system and its boundaries
    - Define the scope of the Risk Assessment Effort
    - Document all pertinent factors
        - Hardware
        - Software
            - Server Farms
        - Internal and external system interfaces
            - .mil and .edu
        - Data and information stored, processed, transferred, and used in the system
        - Support Personnel
        - Users and their organizations
        - The mission of the system
        - The business processes the system performs
        - The value or importance of the system and its data to the organization
        - The classification and sensitivity of the system
        - System flow charts
    - Define Level of Effort
    - Define Mission Assurance Category
- Threat Identification
    - Define all possible circumstances or events that could potentially cause harm to the system
- Vulnerability Identification and Risk Analysis
    - Define all possible Vulnerabilities that could potentially be exploited
    - Describe tools used to detect vulnerabilities
    - Describe the criticality of the system and its data
    - Estimate the likelihood of successful exploitation of each vulnerability
    - Estimate the magnitude of the impact of each attack
    - Assign a level of risk to each potential attack
- Countermeasure Recommendations

    - Countermeasures to mitigate or eliminate the identified risks
        - Technical
        - Non-technical
- Conclusions
- Appendices
- Bibliography
- Initial Distribution List

II. SYSTEM CHARACTERIZATION

A. HARDWARE

The physical design and structure of the NPS network reflects the expansive layout of the campus. NPS has an open campus that consists of over twenty academic, administration, utility, and family housing buildings (See Figure 1). From these buildings, ten academic and administration complexes, the La Mesa Family Housing Center, and the Public Works Complex are connected to the NPS network. The logical design of the network was dependent on the conflicting requirements of the military and university aspects of NPS. Each of the connected buildings contains various amounts and types of hardware and software components that are configured to handle this intricate dichotomy present at NPS.

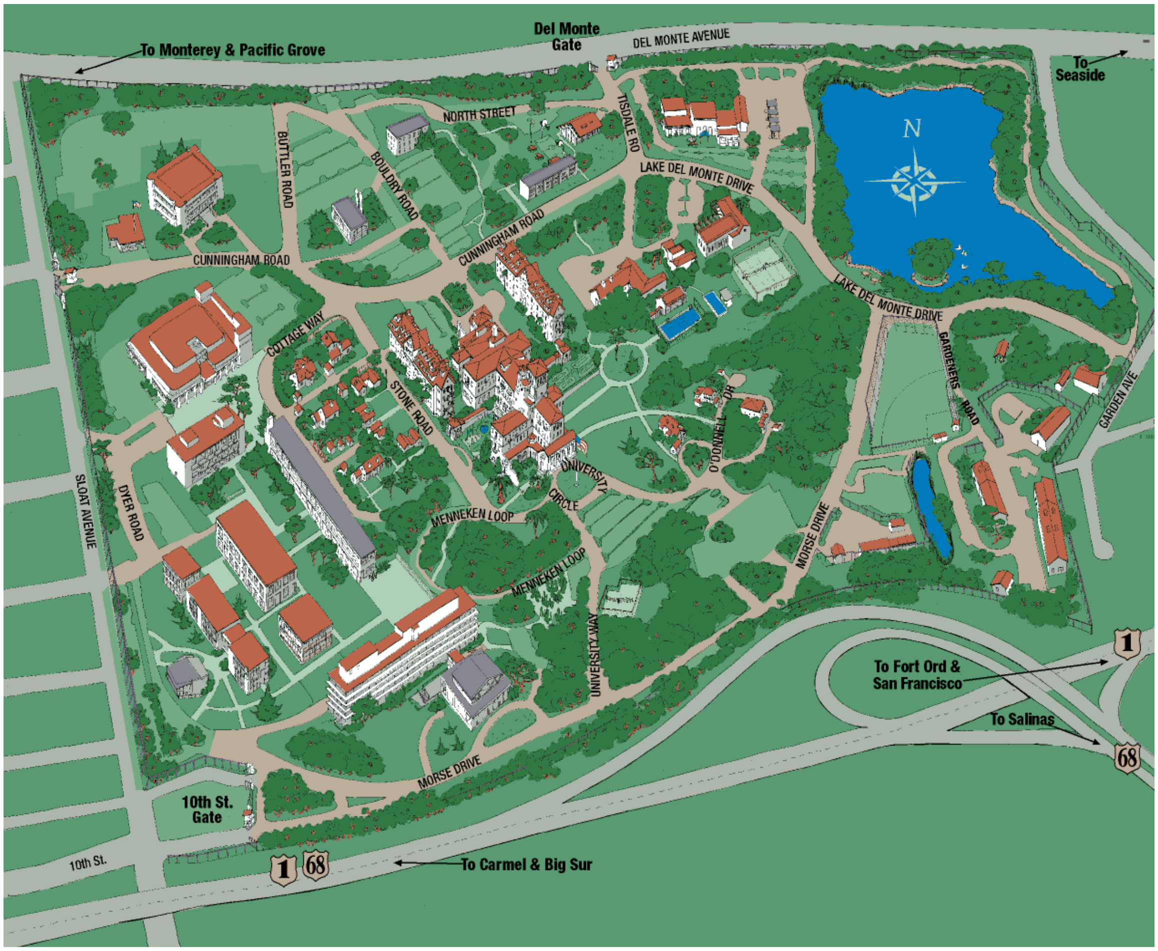

Figure 1. Campus Map

The NPS network was divided into two separate domains, .mil and .edu, in an attempt to satisfy the special requirements that exist from supporting both a military base and a university. The separation was accomplished by creating two distinct external connections to the Internet (See Figure 2) and by partitioning Virtual Local Area Networks (VLANs) throughout the network for both the .mil and .edu hosts. The .mil domain, dedicated to the military needs of NPS, has a Class B IP range with host number 131.120.X.X. The .edu domain, dedicated to the university needs of NPS, has a private IP space and will implement Network Address Translation (NAT) in order to access the Internet. Because of the large number of foreign national students attending NPS, it was necessary to place some type of control on which students were accessing United States government websites containing sensitive but unclassified information. In the future, any person or service that is logged onto a .mil or .edu host will also be required to authenticate at a proxy server that will be located in the DMZ in order to access restricted sites that require a .mil domain name. Also, all communication between the two domains that originates from the .edu domain will be required to authenticate through a VPN/SSL.

The central portion and backbone of the NPS network and the vast majority of the Information Technology staff are located in Ingersoll Hall at the Data Center. All inbound, outbound, and inter-building traffic travels through the hardware in this building. The Data Center contains all of the following hardware components (See Figure 3):

- Three BigIron 8000 backbone switches
- Two BigIron 4000 backbone switches
- One Server farm for each domain comprising of approximately one-hundred and forty servers
- Router Rack
    - .mil domain
        - Two 75xx Cisco Routers
        - Cisco Pix Firewall
        - Two 3Com 3300 Switches
        - Three Intrusion Detection Machines
            - Snortnet (2)
            - Stealthwatch

- .edu domain
  - Cisco 7200 Router
  - Netscreen Firewall

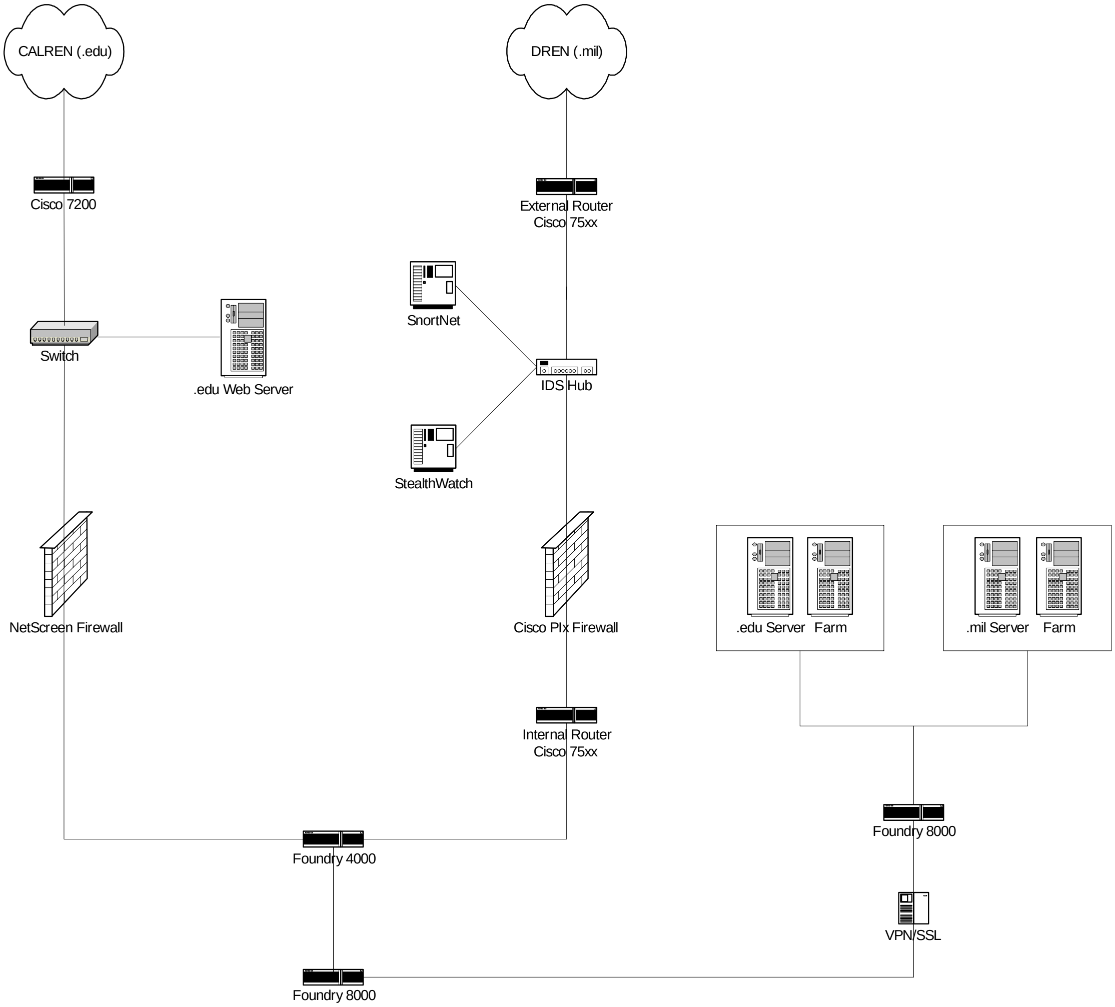

Figure 2. Separate Domains of NPS Network.

The NPS campus network has a three-tiered hierarchy of switch classes that increase in speed and capability as data flows towards the interior of the network. The center of the network consists of the three BigIron 8000 layer three backbone switches, which are the fastest of the switches implemented at NPS. The BigIron 8000 switches are directly connected through fiber optic lines to the twelve BigIron 4000 layer three switches located throughout the campus and to all of the servers in the two Server Farms.

The BigIron 8000 switches are responsible for forwarding all of the traffic on the network, except for intra-building communications, which are handled by the local BigIron 4000 switches in each building.

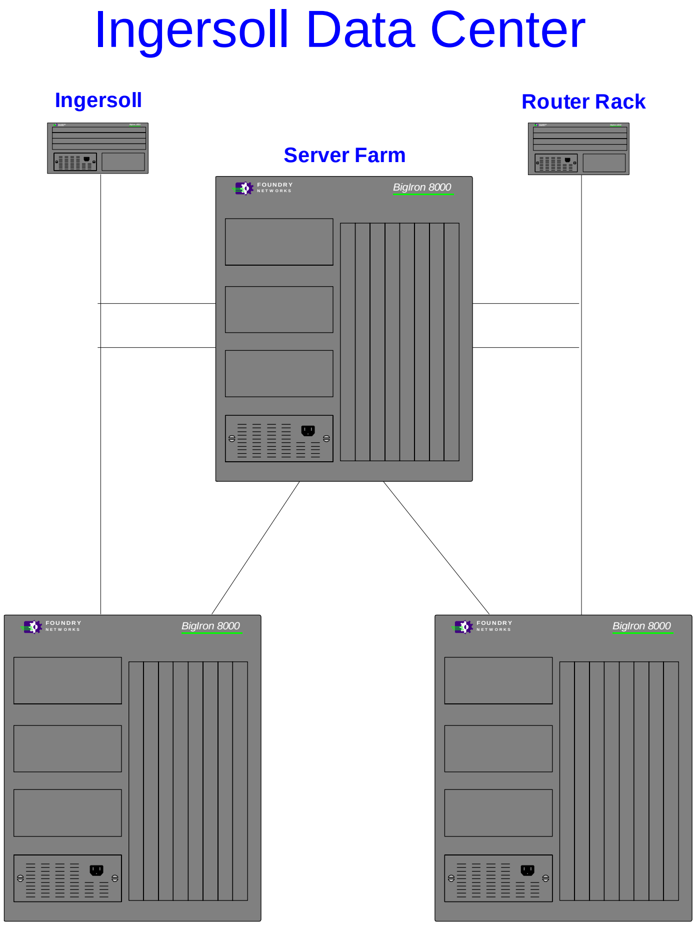

Figure 3. Data Center

The majority of the BigIron 4000 switches are dedicated to either an entire networked campus building, a portion of a networked campus building, or an academic department. There is one BigIron 4000 switch located at all of the network connected academic and administration buildings except for Herrmann Hall, Spanagel Hall, and Ingersoll Hall. Because the Computer Science Department is located in Spanagel Hall and has its own BigIron 4000 switch, this building has two BigIron 4000 switches. There are also two BigIron 4000 switches that divide Hermann hall into two separate VLANs.

The BigIron 4000 switches combine to break the campus network into eleven logically separated VLANs (See Figure 4). The Data Center in Ingersoll Hall, as documented earlier, contains two BigIron 4000 switches. One of these switches is dedicated to communications to and from the router rack and the other BigIron 4000 is responsible for connecting the local host machines as in the other buildings. The La Mesa Family Housing Center and the Public Works Complex are joined to the network as subnets and are directly connected by a fiber optic line to either the gateway router or to one of the BigIron 8000 switches.

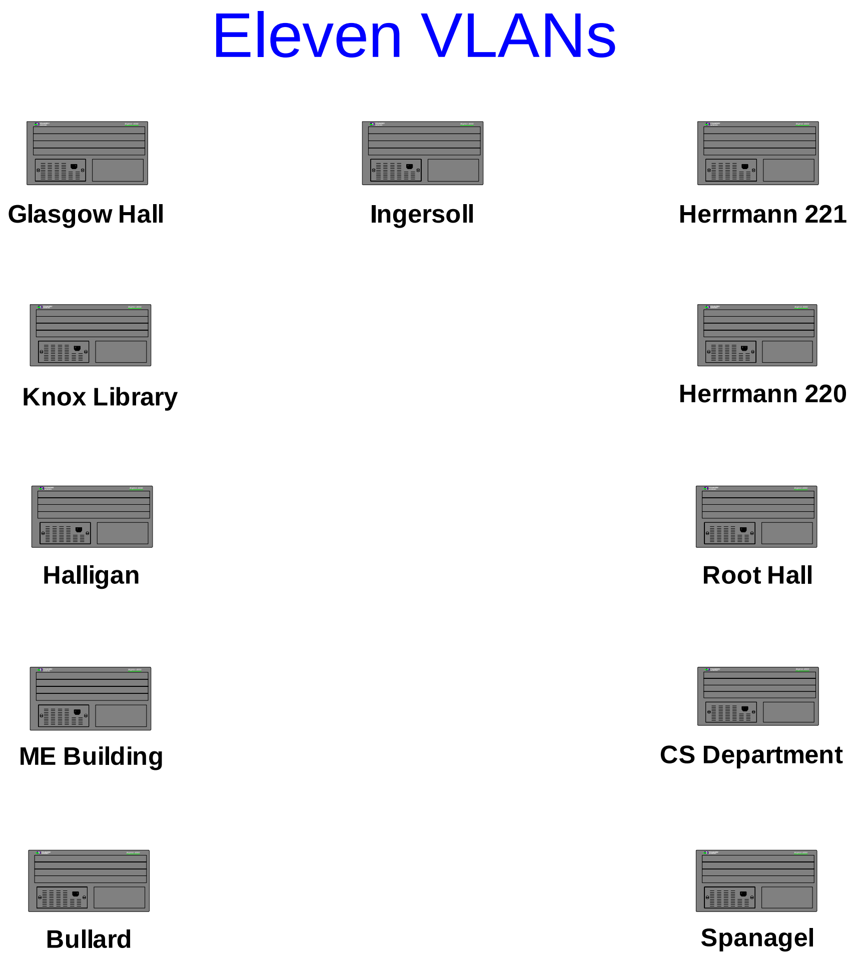

Figure 4. Eleven VLANs.

Each of the BigIron 4000 switches dedicated to a building or department is connected to a series of FastIron Edge 4802 or 3Com SuperStack 3300 layer two switches that separate each building or department into smaller VLANs and connect the host machines of each building to the network. Because each of the connected buildings requires a different number of host machines, there are a varying number of VLANs and FastIron or 3Com switches located in each building. Also, each building has a varying number of VLANs associated with both the .mil and .edu domains. The names of the connected buildings, the number of total VLANs per building, the names of each VLAN, and the exact type and amount of switches per VLAN are as follows:

- Bullard Hall (See Figure 5)
  - 3 VLANs
    - Bullard 100a
      - 1 FastIron Edge 4802
    - Bullard 125
      - 2 FastIron Edge 4802
    - Bullard 212
      - 3 FastIron Edge 4802
- Glasgow Hall (See Figure 6)
  - 7 VLANS
    - Glasgow 0H9
      - 1 FastIron Edge 4802
      - 1 3Com SuperStack 3300
    - Glasgow 2B2
      - 2 FastIron Edge 4802
    - Glasgow 295
      - 3 FastIron Edge 4802
    - Glasgow 2H9
      - 2 FastIron Edge 4802
    - Glasgow 3B2
      - 2 FastIron Edge 4802
    - Glasgow 3B9
      - 2 FastIron Edge 4802
    - Glasgow 3H9
      - 2 FastIron Edge 4802
- Halligan Hall (See Figure 7)
  - 4 VLANs
    - Halligan 028

            - 2 FastIron Edge 4802
        - Halligan 103c
            - 2 FastIron Edge 4802
        - Halligan 201c
            - 2 FastIron Edge 4802
        - Halligan 255
            - 2 FastIron Edge 4802
- Herrmann Hall 220 (See Figure 8)
    - 5 VLANs
        - Herrmann 028
            - 2 FastIron Edge 4802
        - Herrmann 069
            - 3 FastIron Edge 4802
        - Herrmann M8b
            - 3 FastIron Edge 4802
        - Herrmann 136a
            - 3 FastIron Edge 4802
        - Herrmann 416
            - 1 3Com SuperStack 3300
- Herrmann Hall 221 (See Figure 9)
    - 5 VLANs
        - HerrmannE 114
            - 1 FastIron Edge 4802
        - HerrmannE 204
            - 2 FastIron Edge 4802
        - HerrmannE 214
            - 2 FastIron Edge 4802
        - HerrmannE 316
            - 2 FastIron Edge 4802
        - HermmanE 506
            - 1 FastIron Edge 4802
- Herrmann Hall 222 (See Figure 10)
    - 2 VLANs
        - HerrmannW 115
            - 2 FastIron Edge 4802

        - HerrmannW 506
            - 1 FastIron Edge 4802
- Ingersoll Hall (See Figure 11)
    - 4 VLANs
        - Ingersoll 149
            - 4 FastIron Edge 4802
        - Ingersoll 279
            - 4 FastIron Edge 4802
        - Ingersoll 365
            - 5 FastIron Edge 4802
        - CEE Garage
            - 1 3Com 4900SX
            - 8 3Com SuperStack 3300
- King Hall
    - 1 VLAN
        - 1 3Com SuperStack 3300
- Knox Library (See Figure 12)
    - 5 VLANS
        - Knox 109
            - 1 FastIron Edge 4802
        - Knox 152
            - 1 FastIron Edge 4802
        - Knox 169
            - 1 FastIron Edge 4802
        - Knox 209
            - 1 FastIron Edge 4802
        - Knox 265
            - 1 3Com SuperStack 3300
- ME Building (See Figure 13)
    - 3 VLANs
        - ME Garage
            - 1 FastIron Edge 4802
        - ME 2nd Floor
            - 3 FastIron Edge 4802
        - ME Annex

            - 4 FastIron Edge 4802
- Root Hall (See Figure 14)
    - 5 VLANs
        - Root 107c
            - 2 FastIron Edge 4802
        - Root 123
            - 2 FastIron Edge 4802
        - Root 200a
            - 1 3Com SuperStack 3300
        - Root 220
            - 7 FastIron Edge 4802
        - Root 268
            - 2 FastIron Edge 4802
- Spanagel Hall (See Figure 15)
    - 7 VLANs
        - Spanagel 032
            - 2 FastIron Edge 4802
        - Spanagel 132
            - 3 FastIron Edge 4802
        - Spanagel 234
            - 2 FastIron Edge 4802
        - Spanagel 303a
            - 4 FastIron Edge 4802
        - Spanagel 338
            - 5 FastIron Edge 4802
        - Spanagel 440
            - 4 FastIron Edge 4802
        - Spanagel 538
            - 2 FastIron Edge 4802
- Computer Science Department (See Figure 16)
    - 3 VLANS
        - Spanagel 259
            - 4 FastIron Edge 4802
        - Spanagel 500
            - 2 FastIron Edge 4802

- Spanagel 523
  - 2 FastIron Edge 4802

- CEE Garage (See Figure 17)
  - 8 VLANS
    - Qtrs B
      - 1 3Com SuperStack 3300
    - Qtrs C
      - 1 3Com SuperStack 3300
    - Qtrs E
      - 1 3Com SuperStack 3300
    - Qtrs F
      - 1 3Com SuperStack 3300
    - Qtrs G
      - 1 3Com SuperStack 3300
    - Qtrs H
      - 1 3Com SuperStack 3300
    - Qtrs I
      - 1 3Com SuperStack 3300
    - Qtrs J
      - 1 3Com SuperStack 3300
- La Mesa Housing Center (See Figure 18)
  - 5 VLANS
    - Self Help Barn
      - 1 3Com SuperStack 3300
    - Youth Center
      - 1 3Com SuperStack 3300
    - Family Services
      - 2 3Com SuperStack 3300
    - 1283 Leahy
      - 1 3Com SuperStack 3300
    - Community Center
      - 1 3Com SuperStack 3300
- Publics Works Complex (See Figure 19)
  - 5 VLANS
    - Building 427
      - 1 3Com SuperStack 3300

- Building 428
    - 1 3Com SuperStack 3300
- Building 436
    - 2 3Com SuperStack 3300
- Building 437
    - 1 3Com SuperStack 3300
- Building 349
    - 1 3Com SuperStack 3300

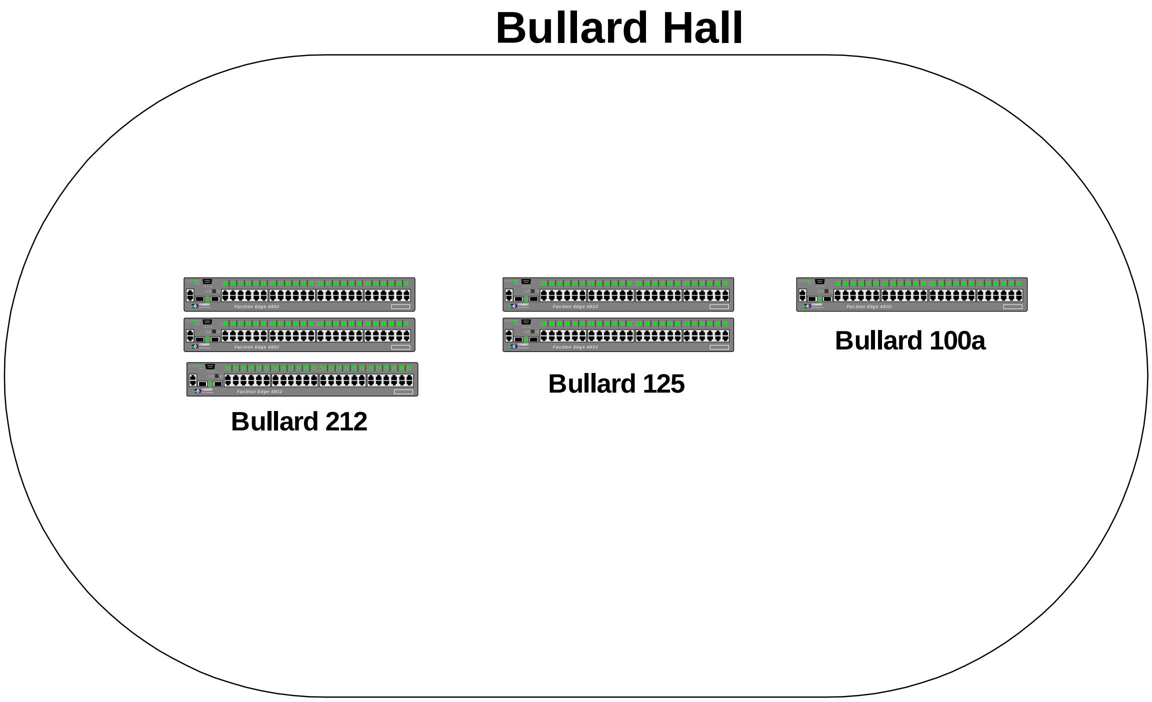

Figure 5. Bullard Hall.

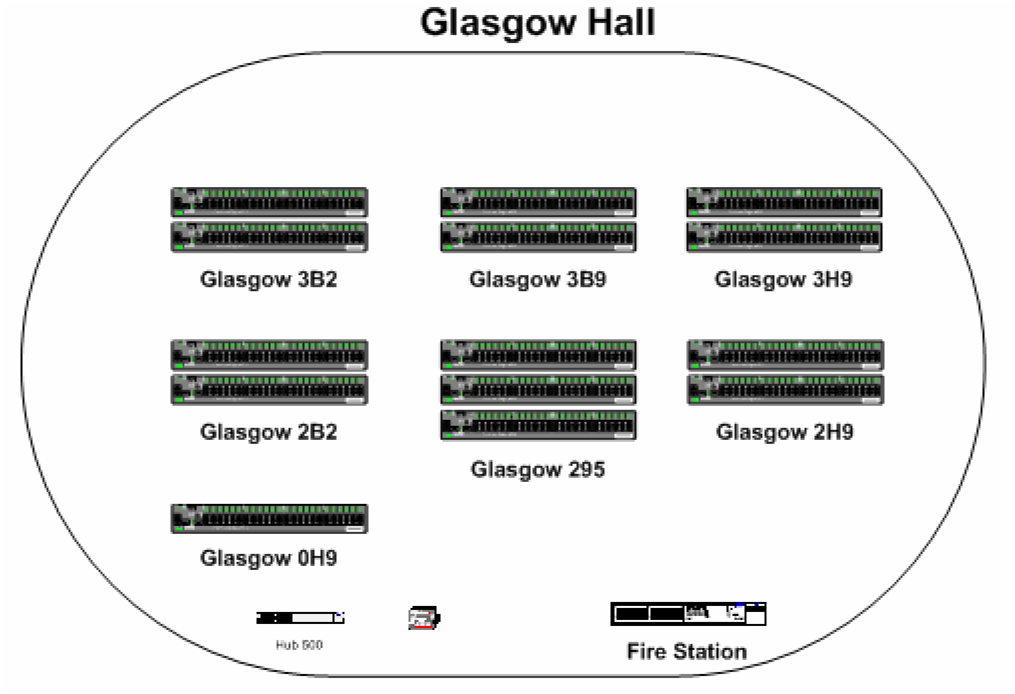

Figure 6. Glasgow Hall.

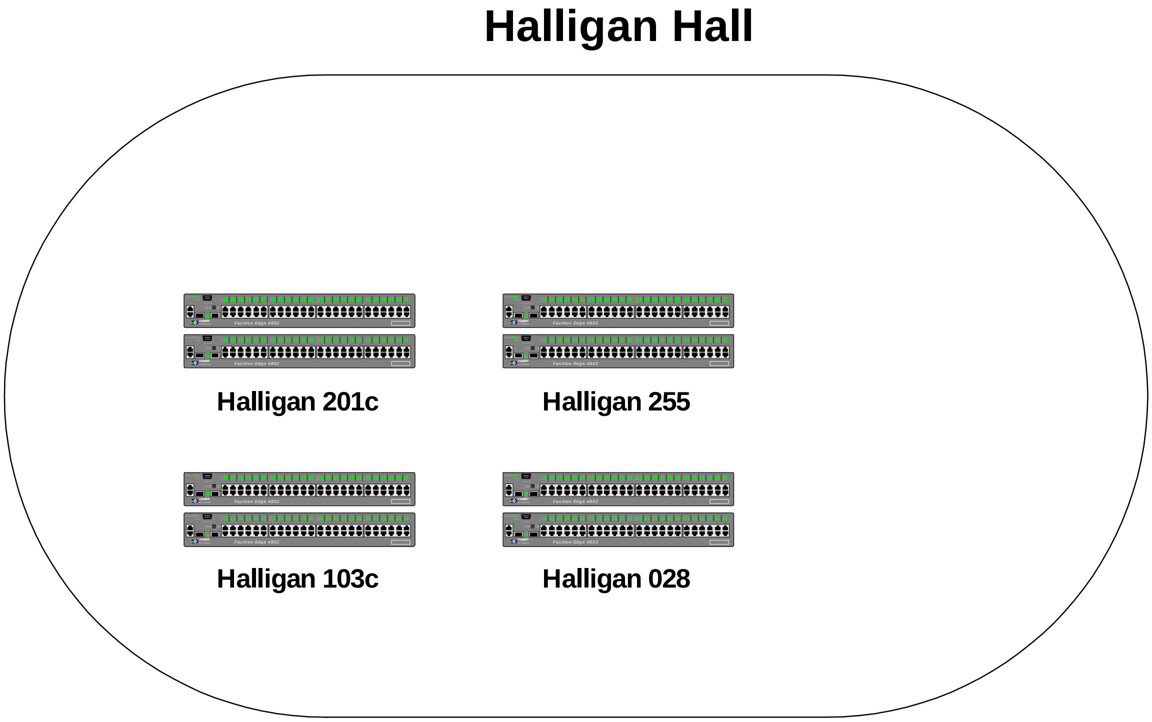

Figure 7. Halligan Hall.

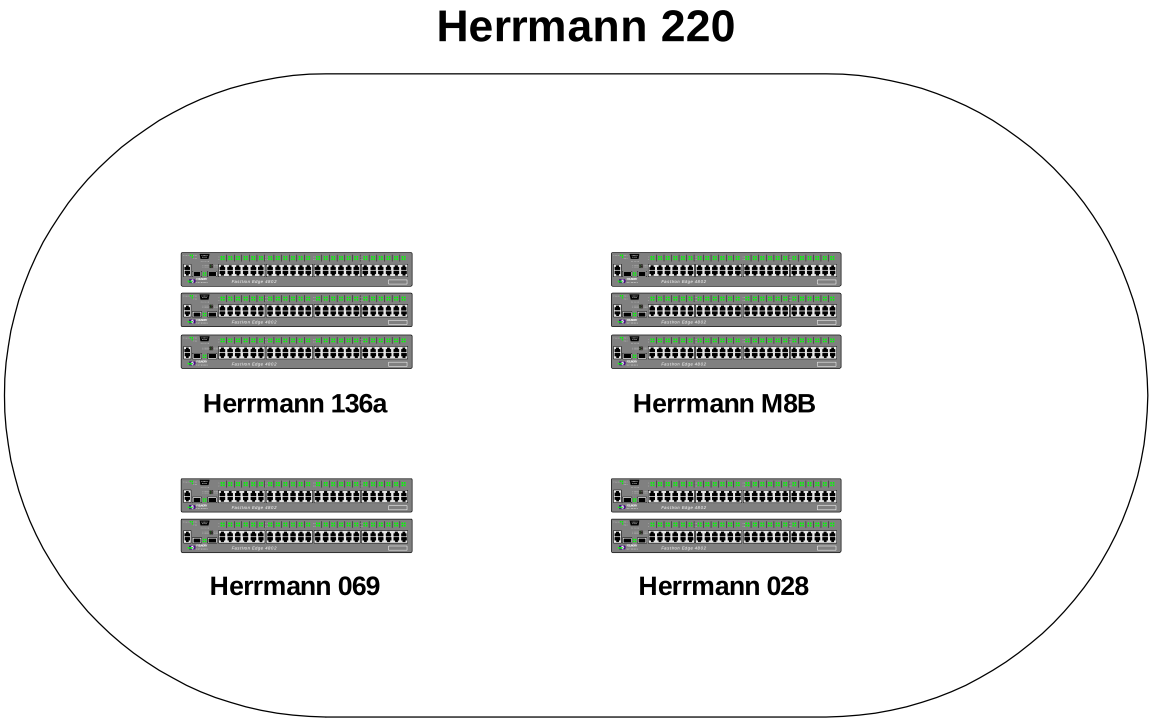

Figure 8. Herrmann Hall 220.

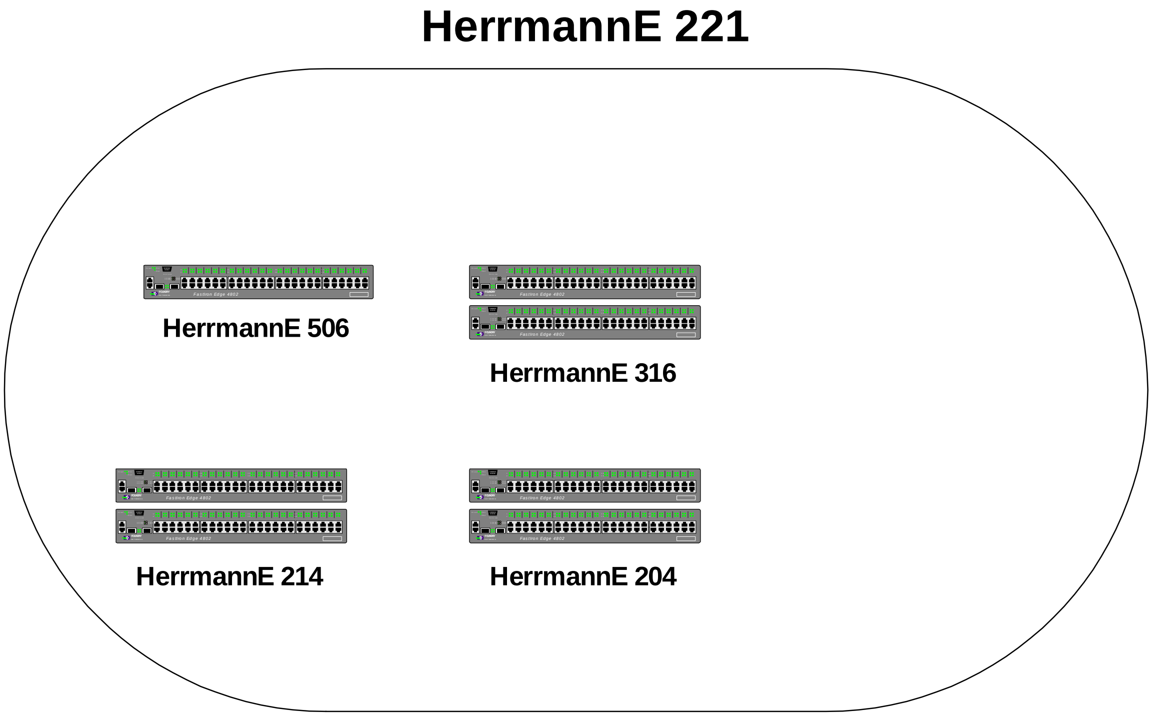

Figure 9. Herrmann Hall 221.

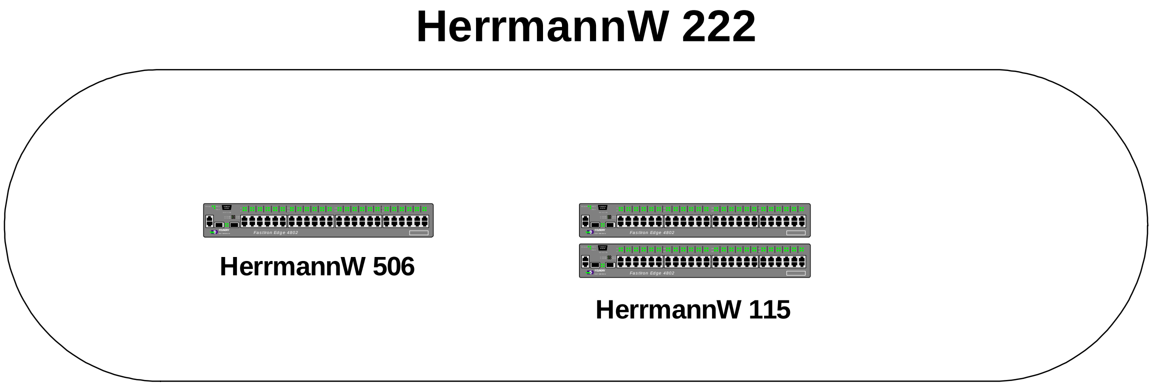

Figure 10. Herrmann Hall 222.

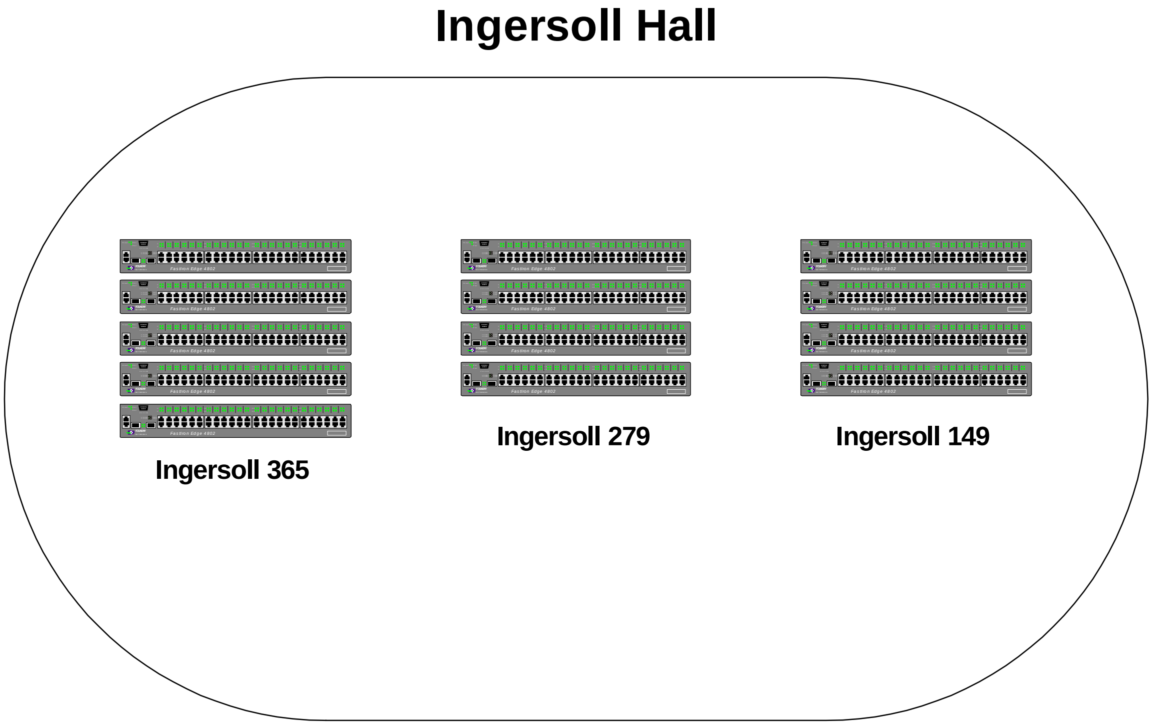

Figure 11. Ingersoll Hall.

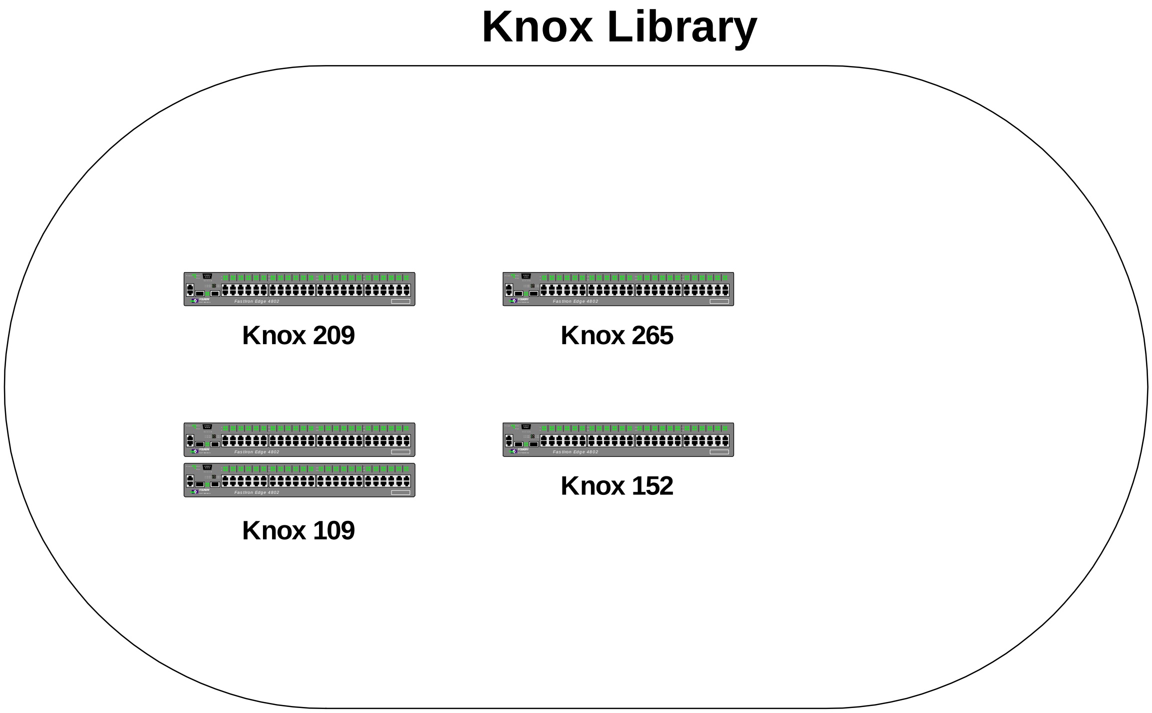

Figure 12. Knox Library.

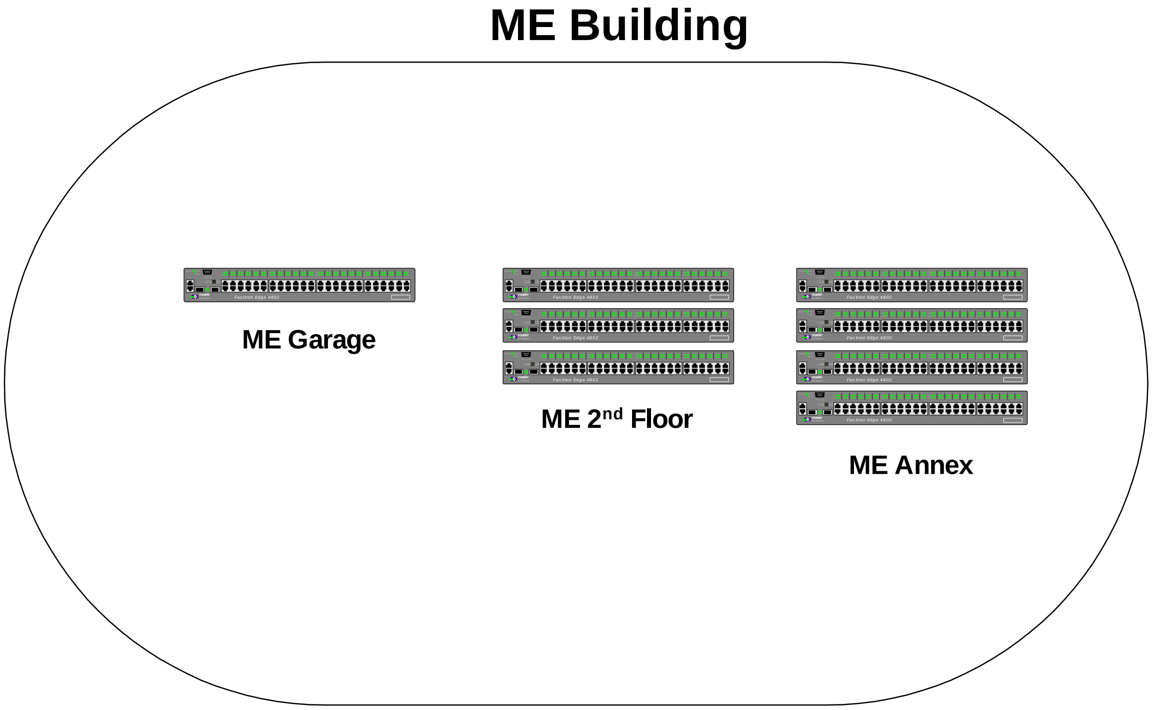

Figure 13. ME Building.

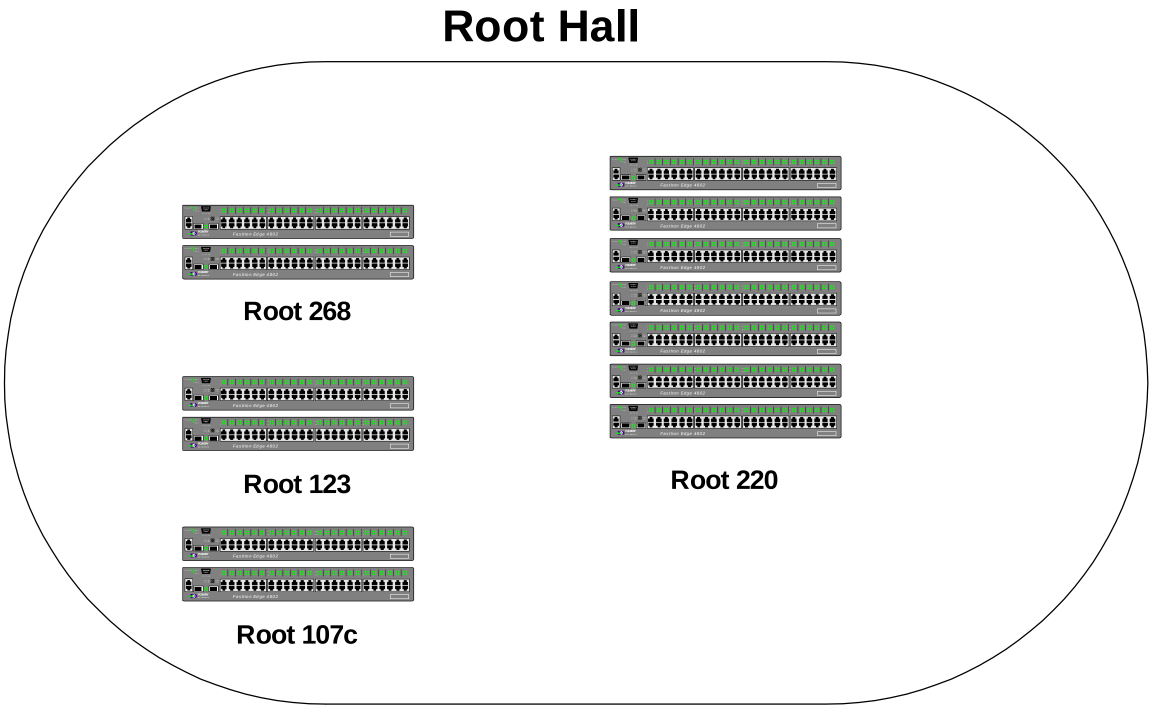

Figure 14. Root Hall.

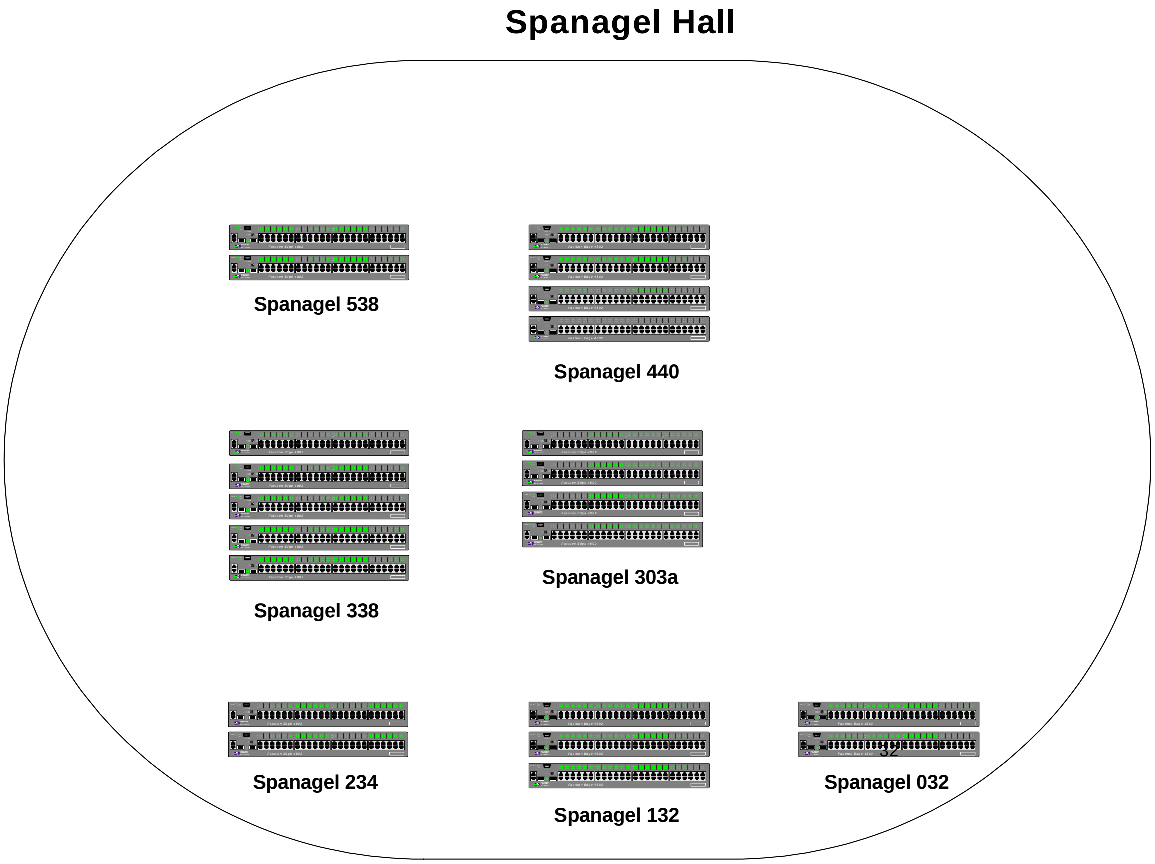

Figure 15. Spanagel Hall.

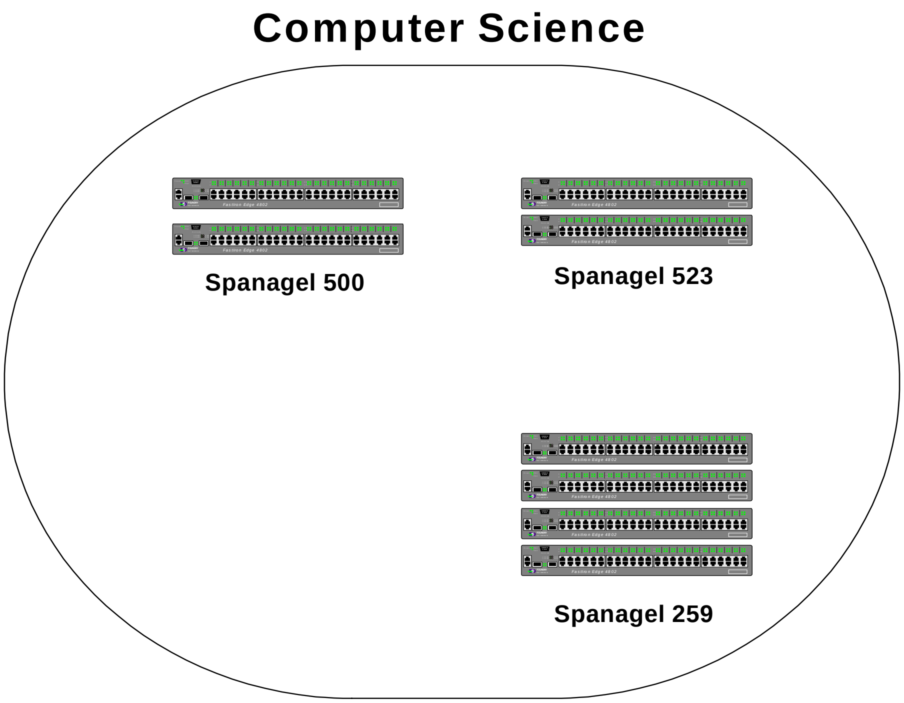

Figure 16. Computer Science Department.

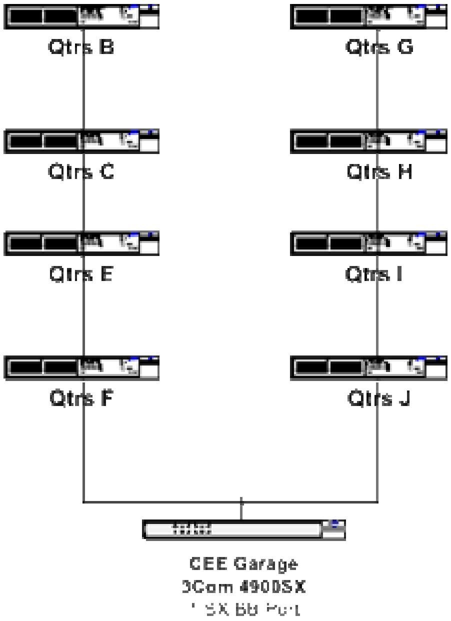

Figure 17. CEE Garage.

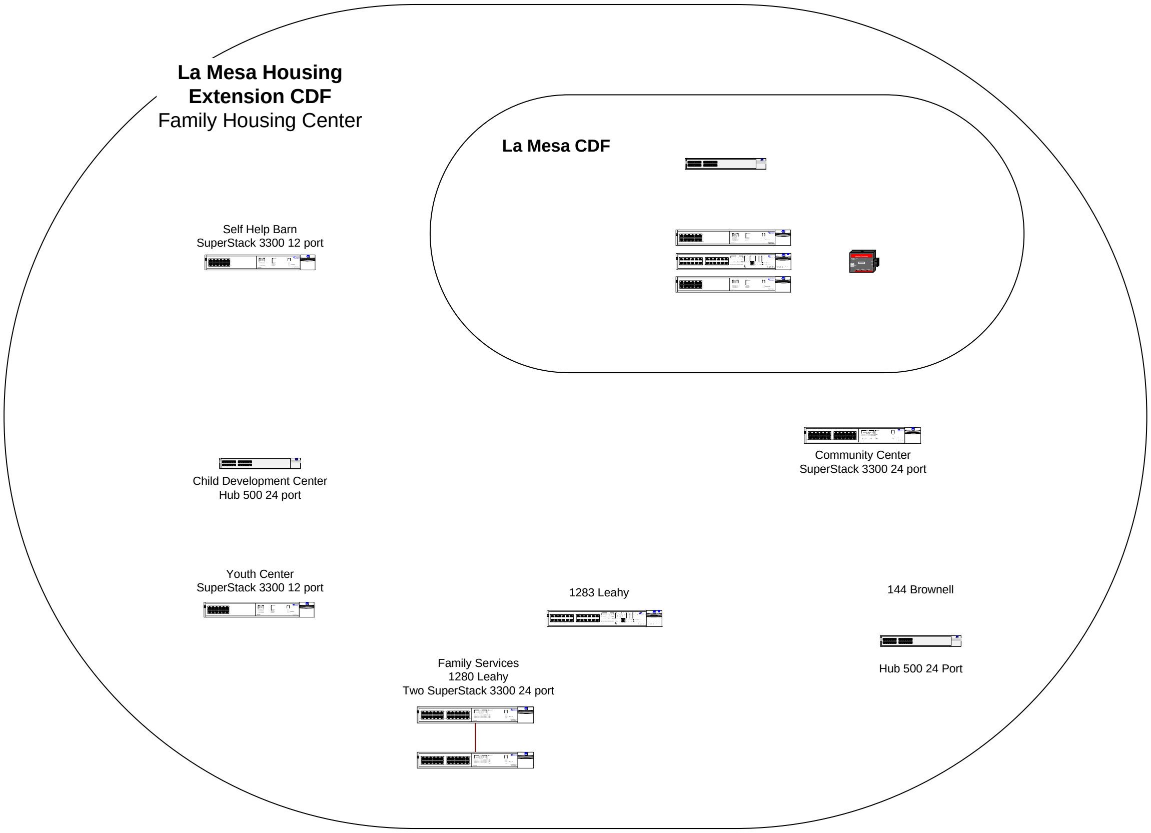

Figure 18. La Mesa Housing Center.

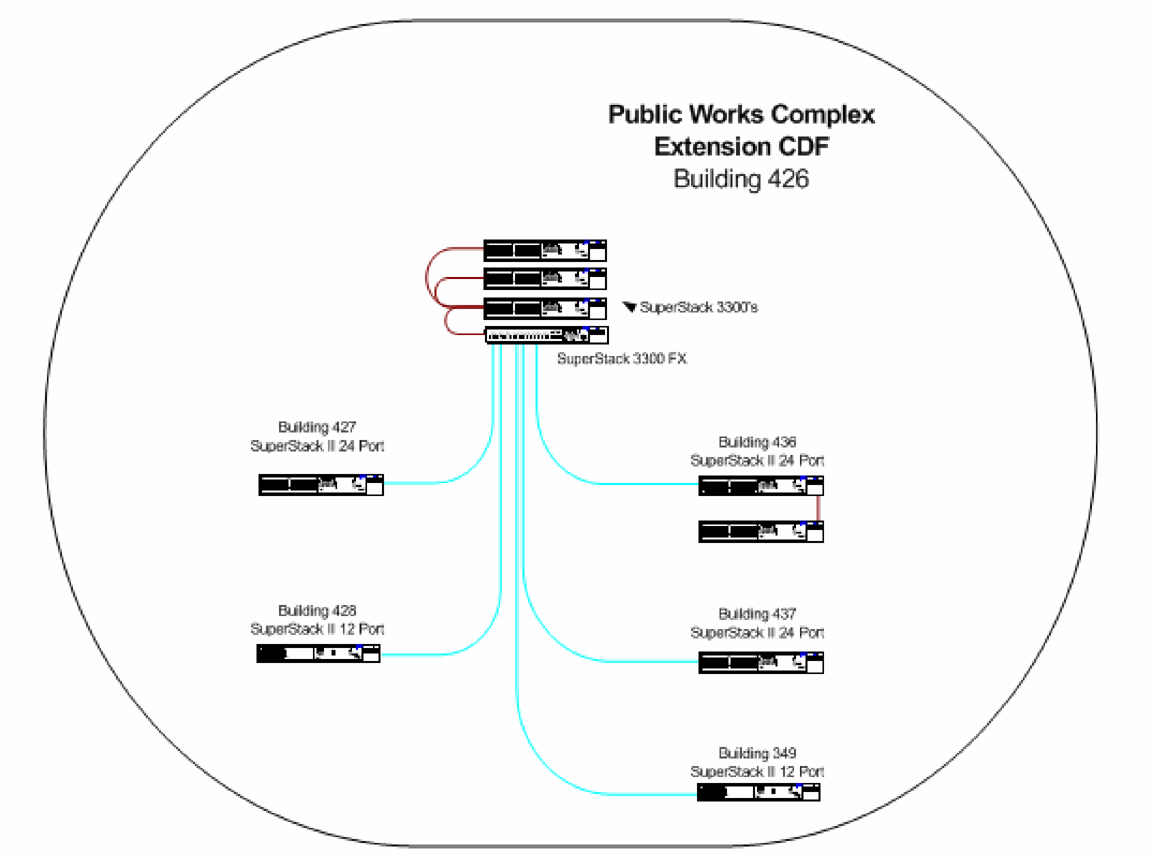

Figure 19. Public Works Complex.

B. SOFTWARE

The current server farm consists of over one-hundred forty servers that are responsible for hosting various applications and services. In the future, the server farm will be split into two distinct server farms to represent both the .mil and .edu domains. However, at the present time all of the servers that make up the campus network belong to one server farm. The server farm is centralized at the Ingersoll Hall Data Center, but there are some servers located sporadically across the campus belonging to various departments, students, or faculty. The overwhelming majority of the servers are running Windows 2000 Server Advanced, Windows 2000 Server, or Windows NT Server 4.0. However, there is a small number of servers running Unix. The following list details the different types and amount of servers attached to the network (See Appendix A):

- Autocad Server (1)
- Backup and Data Restores (1)
- Citrix Servers (7)

- Defense Messaging Server (1)
- Domain Controllers (4)
- DORS Development Server (2)
- EHF Server (1)
- EWS Server (1)
- Exchange Server (8)
- Fastdata Server (2)
- File Servers (8)
- Financial/Accounting Server (1)
- Landesk Server (3)
- Maximo Server (1)
- MS Windows Updater Server (1)
- Network Attached Storage Servers (5)
- Norton Antivirus Servers (3)
- OAPIWeb Server (1)
- Python Web Management Server (1)
- Ras Server (1)
- Remedy Server (1)
- Samba Server(2)
- SQL Servers (3)
- Web Servers (3)
- WINS Server (1)
- Library Management Servers (6)
- Miscellaneous Servers (64)

C. EXTERNAL AND INTERNAL CONNECTIONS

The partition of the Naval Postgraduate School campus network into two separate domains has necessitated two distinct external network connections and an internal connection to handle communications between the two domains. The .mil domain has an external connection to the DREN network and the .edu domain has an external connection to the CALREN network. The internal connection between the two domains will be handled by a VPN/SSL that will manage communications from one domain to another via an Active Directory type access control mechanism.

The creation of two separate external connections has also caused the need for multiple sets of security mechanisms to protect and monitor both domains. The filtering capabilities of the external gateway routers for both domains provide the first level of defense from both outside and inside threats. For the .mil domain, a Cisco Pix firewall has been implemented to mediate all inbound and outbound traffic to the DREN network. Also, there are two separate intrusion detection systems, Snortnet and Stealthwatch, located on a mirrored port that dynamically examine all communications entering and exiting the .mil domain. For the .edu domain, there has been a Netscreen firewall employed to filter the inbound and outbound traffic to the CALREN network. The .edu web server is positioned in the DMZ and is located inside the external gateway to CALREN, but outside the Netscreen firewall. The web server will be adequately hardened to protect itself from any malicious outside communications that would normally be detected and filtered by the firewall.

The .mil firewall, .edu firewall, and the VPN/SSL that mediates communications between the two domains must adhere to the rules described in the Navy-Marine Corps Unclassified Trusted Network Protection policy (UTNProtect). The policy dictates that all firewalls protecting trusted Navy or Marine Corps networks must implement a deny-by-default posture. The policy also lists a minimum set of baseline firewall configuration settings that determine what services, ports, and protocols are authorized for transmission from a trusted network to an untrusted network. The baseline settings are not to be used as a default and the DAA for each site must determine if all of the settings are necessary (See Appendix A). Because both the .mil and .edu domains adhere to the UTNProtect policy, special permission does not need to be given by CNO N6/HQMC C4 prior to the implementation of the VPN/SSL. However, all VPN requests between the two domains must be in accordance with the baseline settings detailed in the policy. Because the NPS campus network is a Navy-Marine Corps Intranet connected system, the UTNProtect policy is comprehensive enough to encompass all of the Ports, Protocols, and Services policy.

The Defense Management Data Center (DMDC) located at Fort Ord is joined to the NPS campus network as a subnet and has a direct connection to the external router of the .mil domain. DMDC currently accesses the NPS campus network through this subnet for two separate applications. The DIRS application communicates with several servers at NPS to deposit and query information. Currently, this communication is sent back and forth in the clear without the implementation of a VPN. The BIDS application also communicates with several servers at NPS, but a VPN is used to encrypt data in transmission. The host machines at DMDC that are connected to the NPS subnet are housed inside a facility with strict physical security. No access is permitted inside the building without the escort of a cleared DMDC employee. Therefore, it is extremely unlikely the NPS host machines located at DMDC will be accessed by improper personnel.

D. SYSTEM CRITICALITY

The Naval Postgraduate School campus network provides students and faculty the resources required for education and research. Each student and member of the faculty is allocated a network account, which includes data storage and use of software applications for various tasks such as word processing, presentations, creation and compilation of programs, and any other reasonable tools necessary for the learning process. The campus network also provides students and faculty a connection to the Internet to perform research and utilize information found outside of the .mil or .edu domains. Because of the benign nature of the activities performed by the users of the NPS network, all data posted or displayed at NPS is categorized as unclassified.

Users of the NPS network are either members of the faculty, NPS employees, or military or civilian students. Each user must be granted access to the system on an individual basis by the proper system administrators. Because of the data classification level, a special clearance is not required. However, if a clearance is required it will be set by the proper corresponding departement at NPS. The large number of foreign military students has created the need to mediate access to government websites that contain need-to-know information. To obatain an IP address from the .mil class B pool that would allow access to sensitive government sites, a user must either be logged on to a

.mil host machine or pass through the access control mechanism of the VPN/SSL. Also, in the future, each user on either the .mil or .edu domain will need to authenticate through a proxy server to gain access to sites that require a .mil domain name.

The NPS network has a Mission Assurance Category (MAC) III rating. The system handles information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. As discussed, the classification level of data located in the NPS network is unclassified. Also, a compromise of the NPS campus network would not result in the loss of life, injury, or severely hinder the overall mission of the Naval Postgraduate School. The most damaging consequence of a successful attack against the NPS network would be the resulting negative impact to the reputation of the Department of the Navy, Department of Defense, and in turn, the competency of the United States Government. For this reason, the NPS campus network requires a MAC III rating as opposed to being labeled an administrative or mission support site.

E. CONTINGENCY PLAN

The Tivoli Backup and Recovery Storage Manager has been implemented to serve as the system backup tool for the NPS campus network. The Tivoli manager by default performs backups with a system known as one full and incremental forever. With this system, Tivoli will create a full backup the first time a particular server or file is scheduled for backup. After the first time, an incremental backup is performed for the remainder of the time the server is associated with Tivoli. However, the Tivoli manager at NPS has been configured to perform a new full backup on a monthly basis. The amount of incremental backups saved by Tivoli is completely dependent on the policy that was created for the particular file or server by the system administrator. Once the threshold dictated in the policy for a file or server has been reached for incremental backups, the oldest incremental backup is discarded.

At NPS, the Tivoli manager is running on the NDSM1 server that has a connection to both the NPS campus network and the server where the backups are cached until written to tape. The server responsible for caching the backups has a terabyte capacity that is distributed over five physical disks. The write to the taped backups is triggered by either reaching the predetermined capacity threshold for one of the physical disks or the daily schedule maintained by the Tivoli manager (See Figure 20). Currently, there is no offsite storage for completed backup tapes.

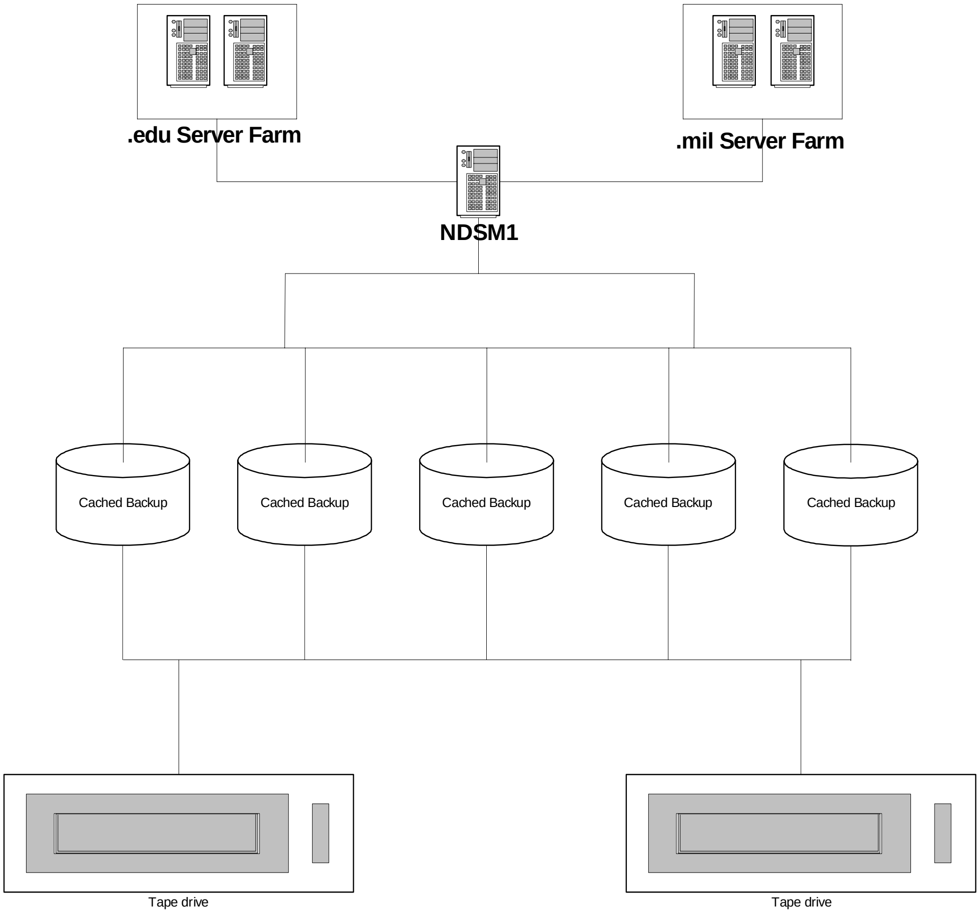

Figure 20. Tivoli Manager.

F. LEVEL OF EFFORT

The level of effort measurement was determined by examining seven system characteristics of the NPS campus network. The measurement will be used to establish both the density of security safeguards needed to adequately protect the system and the amount of resources required to provide the DAA with a sufficient amount of information about the system to make an accreditation decision. The seven characteristics included in the level of effort are as follows:

- Interfacing Mode
- Processing Mode
- Attribution Mode
- Mission Reliance
- Availability
- Integrity
- Information Categories

Because the Naval Postgraduate School is an academic institution, most of these categories received a very low rating. For example, the integrity and availability of the network do not significantly impact the ability of the school to continue educational procedures. However, because the NPS network interacts with both the DREN and CALREN networks, the interfacing mode received the highest possible rating (See Table 1). After calculating scores for each of the characteristics, the total score combined with the necessity to protect the reputation of the school yielded the requirement for basic assurance. The basic assurance rating dictates that the NPS campus network should implement at minimum the following safeguards:

- Minimal Security Checklist
- Auditing
- Access control
- Identification and Authentication
- Network vulnerability tool
- EAL 1 or 2 rating
- Small amount of documentation and resources dedicated to information security
- Documentary and test evidence

Characteristic	**Alternatives and Weights**	**Weight**
Interfacing Mode	Benign	6
Processing Mode	Dedicated	1
Attribution Mode	Rudimentary	1
Mission-Reliance	Cursory	1
Availability	Reasonable	1
Integrity	Approximate	3
Information Categories	Unclassified	1
	Total of all weights	**14**

Table 1. Basic Assurance Rating.

G. SUPPORT PERSONNEL

The NPS campus network is supported and maintained by three separate departments. The Network Operation Center department is responsible for the day-to-day operations of every aspect of the network. The Infrastructure department is responsible for installing cabling and access ports and for any small remodeling projects that may occur. The Security Department and Network Security Group closely interact with the other departments to ensure that the proper security mechanisms are implemented and working correctly. Also, the Security Department performs defensive tasks such as vulnerability scanning and assessments. The breakdown of personnel for each department is as follows:

- Network Operations Center
  - 7 employees
- Infrastructure Department
  - 2 employees
- Security Department
  - 2 employees

III. THREAT IDENTIFICATION

A. OVERVIEW

The diverse demographics of the user population and the dynamic geographic location of the Naval Postgraduate School present the campus network with some unique threat possibilities specific to NPS. Because many of the students that attend NPS are military members of foreign countries, the likelihood and magnitude of a malicious insider attack increases dramatically. Also, NPS is located on the California shoreline, which drastically increases the chances of both a substantial earthquake and ocean swells that could cause damaging flooding. In the event of these threats coming to fruition, the likelihood of other potential threats, such as power loss and system failure, also increases.

There are also many threats to the NPS campus network that are not unique and that are present in nearly all DoD systems. NPS is a United States government funded university and is therefore a potential target of terrorist groups and political activists that carry a grudge against the country. Also, NPS must mitigate the risk associated with human error and negligence in the same manner as any other DoD system. These are just a few of the many possible threats facing NPS that must be both acknowledged and diminished through the implementation of security safeguards. The following is a list of potential threat categories present at NPS that will be further examined:

- Insider threat
- Outsider threat
- Environmental events
- Support Breakdown

B. INSIDER THREATS

The term insider refers to any authorized personnel who may have access to the NPS network and an insider threat refers to any potential compromise, unauthorized use, or negligence performed by an NPS insider. Because insiders have clearance to interact with the system for some valid reason and are not required to circumvent either the physical security and/or the identification and authentication mechanisms, the insider threat is the most difficult threat to defend against. Also, because insider threats encompass both intentional and non-intentional misuse of the network by insiders, it is the most common threat. As of July 2004, there were 1581 students attending NPS and utilizing the campus network. Of those 1581 students, two-hundred and eighty-six of them were military members of allied countries. There is also another approximately two-hundred employees of NPS that are either support personnel or faculty. In whole, there are nearly 2000 people possessing various technical and ethnic backgrounds that fit the description of an NPS insider.

Insider threats can exist for various reasons and are not required to be malicious in nature. In general, there are four main reasons why insider threats may be present for any given system. They are as follows:

- Ignorance
- Carelessness
- Disregard for policy
- Maliciousness

Ignorance becomes an issue when an insider either does not understand or know about the existing policies. For example, a new employee may unknowingly break the information security policy by setting the password for a system account to an unacceptable length. Carelessness occurs when an insider is aware of the security policy, but does not consider how certain actions would bypass the intent of the policy. Disregard for policy refers to the situation when an insider is fully aware of the policy and cognizant of the ramifications of certain actions that bypass the policy, but continues to perform those actions in an effort to increase ease of use and productivity. For example, an insider may write a password on a piece of paper and be fully aware that the action is a violation of policy, but nevertheless continue to do so to make the task of logging on easier. The previous three reasons carried no inherent bad intentions and would be performed from either a lack of knowledge or to make a task less cumbersome. Maliciousness occurs when an insider purposely sets out to break the information security policy and inflict damage to the system for personal, political, or financial gain.

Insider threats exist at NPS for each of the previously mentioned four reasons. The information security policy is not presented as mandatory reading material for all new incoming students or faculty. For this reason, it is easy to see how ignorance could be a potential problem for the campus network users. Also, the students, faculty, and support personnel at NPS have varying amounts of information technology expertise and at the present time, there are no mandatory courses or training seminars required to increase the awareness and ability of the network users. For the insiders that have had the opportunity to read the policy and the technical ability to understand it, the threats for both carelessness and disregard for policy still exist. As in any setting, the only way to educate insiders about the potential dangers of actions that bypass the intent of the information security policy is through training. There is currently no mandatory information security training present at NPS. Even if there were such training courses, there is no way to guarantee the network users would then decide to adhere completely to the policy.

The threat of a malicious insider attack on the NPS campus network is elevated because of the high number of international students that attend NPS. While all of the international students are military members of allied forces, it is still extremely difficult to screen a potential system user and uncover a hidden agenda when much of the student’s history has taken place in another country. For the most part, all the members of the United States military that are attending NPS have dedicated many years of their career to the country and would not jeopardize their country or career by intentionally damaging the campus network or breaking the information security policy. This being said, there is always the chance that an American military member could become disgruntled and seek revenge by damaging the campus network. Also, there exist the potential for an NPS insider to be recruited by a rogue colleague or foreign intelligence source and either damage the network or provide access to data or computational capabilities. The same possibilities for discontent holds true for the faculty and support personnel at NPS. The following is a list of specific potential insider threats that exist for the NPS campus network:

- Installation of Malware
    - Trojan Horse programs
    - Worms
    - Back doors
    - Rootkits
- Denial of Service
- Theft or disclosure of data
    - Packet Sniffing
- Unauthorized use of software
- Use of system resources for illegal acts
- Use of system resources for personal profit
- Abuse of access controls
- Abuse of power
- Physical theft or destruction of resources
    - Unauthorized use of hardware
- Fraud

C. OUTSIDER THREAT

The term outsider refers to any person that is not authorized to access the NPS campus network either physically or logically. The term includes any person that is not formally approved to pass through the physical security or to remotely log on to the network from an outside system. Any person that is granted access through the physical security, whether or not it is possible for them to log on to the network once inside is irrelevant, is considered an insider. Again, because NPS is a government funded university and a graduate school closely affiliated with the Department of Defense and the Department of the Navy, there is no shortage of candidates available to attempt an outside attack. The following is a list of potential outsider threats to the NPS campus network:

- Hackers
    - Professional
    - Amateur

- Criminals
    - Organized crime
- Terrorists
- Spies
- Political Activists
- Former employees
- Media

There are many ways for an outsider to bypass security mechanisms put in place successfully to protect the network. Also, many of these techniques are completely legal when performed in isolation. For example, an outside attacker could easily obtain valuable information about the network through web research, network scanning, and DNS table examination. Once this data has been assimilated, the attacker can create a profile of the network and begin to locate points of weakness. After the weaknesses have been located, there are hundreds of potential actions the outsider attacker could perform to steal information, decrease network performance, or bring down the network altogether. The following is a list of potential broad attack or action an outsider threat could attempt:

- Installation of Malware
    - Trojan Horses
    - Worms
    - Back doors
    - Rootkits
    - Denial of service
- Theft or disclosure of data
    - Packet sniffing
- Buffer overflow
- Escalation of privileges

D. ENVIRONMENTAL EVENTS

The Naval Postgraduate School is located in Monterey California and is positioned between two of the most active fault lines in the world. Recently, a scientific group known as WG99, which is composed of a large number of experts in the area of earthquakes, made a less than promising diagnosis concerning the long-term stability of the San Francisco Bay area. NPS sits directly between the San Andreas and San Gregorio fault lines and would adversely feel the effects of a strong earthquake in the region. The study performed by WG99 predicts that the Monterey Bay area has a twenty-five percent chance to be victimized by at least one 6.7 magnitude earthquake in the next twenty-five years (See Figure 21).

Recently, there have been several earthquakes around the world of this size that may help predict the amount of damage that will occur in the event of a major earthquake in the Monterey Bay area. A 6.7 magnitude earthquake struck Los Angeles, California, in 1994 and killed fifty-seven people, injured nine-thousand more, destroyed many buildings, and damaged much of the underlying infrastructure in the city. In 1995, an earthquake of similar size killed six-thousand people and completely destroyed a city in Kobe Japan. In short, an earthquake of this magnitude in the Monterey Bay area could destroy buildings and infrastructure, and kill people that are crucial for the NPS campus network to operate and maintain information.

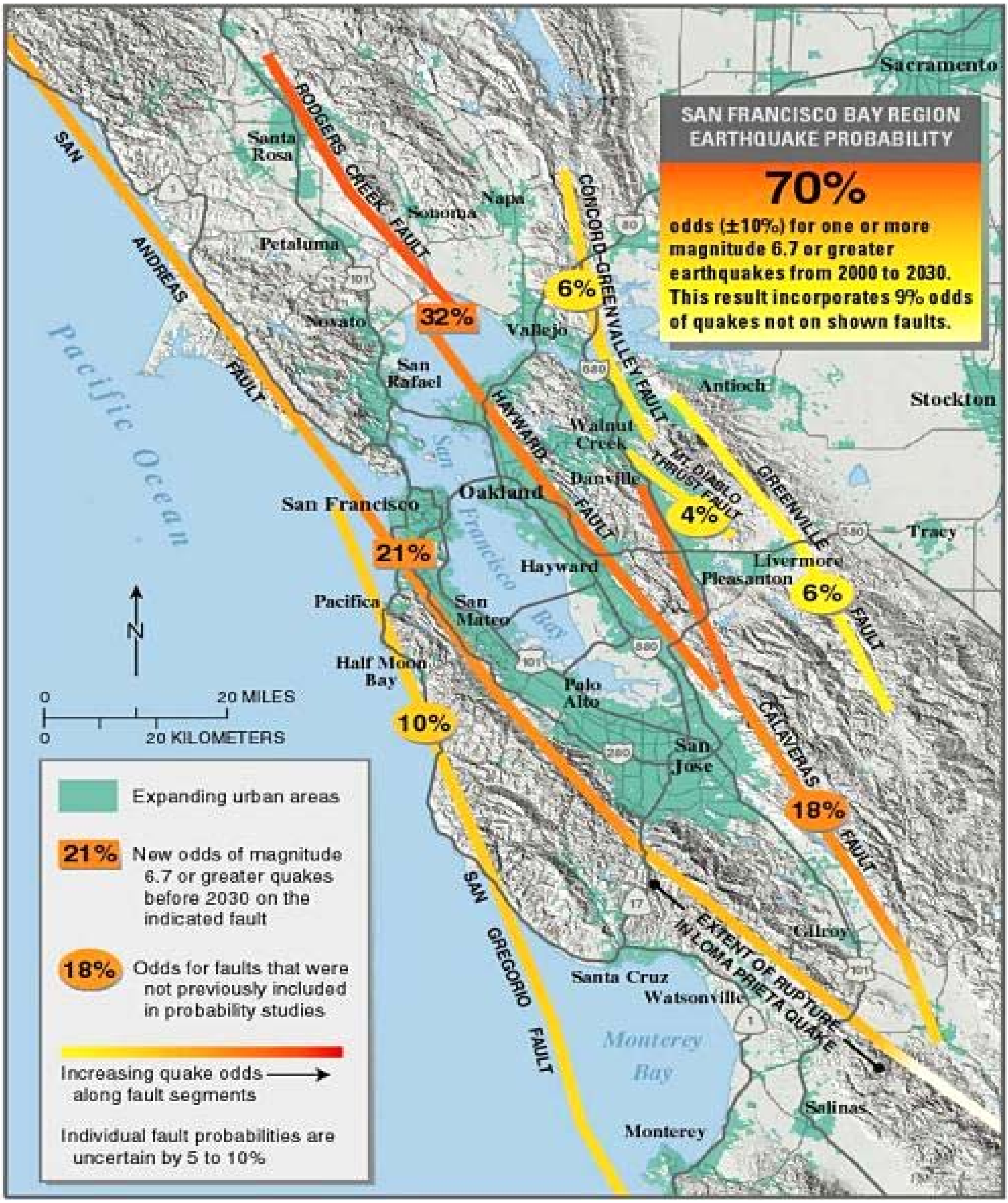
SAN FRANCISCO BAY REGION EARTHQUAKE PROBABILITY
70%
odds (±10%) for one or more magnitude 6.7 or greater earthquakes from 2000 to 2030. This result incorporates 9% odds of quakes not on shown faults.
Sacramento
Santa Rosa
Napa
Sonoma
Petaluma
Novato
San Rafael
Vallejo
Antioch
Stockton
Walnut Creek
Danville
Oakland
San Francisco
Hayward
Livermore
Pleasanton
Tracy
Pacifica
San Mateo
Half Moon Bay
Palo Alto
San Jose
Gilroy
Santa Cruz
Watsonville
Salinas
Monterey
Pacific Ocean
San Francisco Bay
Monterey Bay
SAN ANDREAS FAULT
RODGERS CREEK FAULT
CONCORD-GREEN VALLEY FAULT
HAYWARD FAULT
MT. DIABLO THRUST FAULT
GREENVILLE FAULT
CALAVERAS FAULT
SAN GREGORIO FAULT
EXTENT OF RUPTURE IN LOMA PRIETA QUAKE
32%
6%
21%
4%
6%
10%
18%
N
0
20 MILES
0
20 KILOMETERS
Expanding urban areas
21% New odds of magnitude 6.7 or greater quakes before 2030 on the indicated fault
18% Odds for faults that were not previously included in probability studies
Increasing quake odds along fault segments
Individual fault probabilities are uncertain by 5 to 10%

Figure 21. San Francisco Bay Region Earthquake Probability. [From: Ref. 2]

Another cause for concern in the Monterey Bay region is flooding. The most likely cause of flooding comes from surface runoff during times of heavy seasonal rain. Because over ninety percent of rainfall in the Monterey Bay area occurs between November and April, flooding is usually only a seasonal hazard. However, there are two major dams located in the area and if they failed in the event of a large earthquake, there could be catastrophic flooding. Because NPS is located so close to the Pacific Ocean, earthquakes are also responsible for other types of flooding. While they are much more likely to occur on islands such as Hawaii, a tsunami could possibly bury NPS with enormous waves of ocean water or cause ocean swells that would flood the surrounding area. All of these flooding situations could temporarily shut down the NPS campus network, or worse yet, destroy hardware that is vital to the ability of the network to maintain data.

E. SUPPORT BREAKDOWN

The state of California has a population of over thirty-three million and represents approximately twelve percent of the entire population of the United States. Because of the massive number of people living in California and the extremely hot climate in some portions of the state, there is often a drain on the energy supply. This situation has caused the need for sporadic rolling blackouts during the hot summer months when air conditioners across the state are running at a steady rate. The California Independent System operator, who is in charge of the power supply in the state of California, issues a notice for an energy load reduction to the Californian utility companies. The utility companies are then forced to reply by temporarily shutting the power down in blocks located in their areas for various amounts of time until the state power supply reaches an acceptable level.

The energy crisis and high probability of a blackout situation in California could cause the NPS campus network severe problems during years that are exceptionally hot. A blackout lasting longer than the time the network can run on auxiliary power could be disastrous to the campus network. Also, the high probability of an earthquake also significantly increases the likelihood of a substantial blackout. Because of these situations where blackouts seem inevitable, it is imperative that NPS implement an impeccable policy to deal with the loss of power.

IV. VULNERABILITY IDENTIFICATION

A. OVERVIEW

A vulnerability is a flaw or weakness in an information system, system security procedures, internal controls, or implementation that could be exploited, either accidentally or intentionally, and result in a security breach or violation of the system's security policy. Identifying vulnerabilities in a system as large as the NPS network is a daunting task, but a thorough investigation of the vulnerabilities present must be done in order to assure the aggregate risk of the network is being determined during the risk assessment process.

Identification of vulnerabilities can be done at any point in a system's lifecycle, and depending on where a system is in its lifecycle, the types of vulnerabilities and the methods used to determine their presence are different. Since the NPS network, during the writing of this document, is in a state of flux while being split into the .mil and .edu domains, it is difficult to determine its exact life cycle stage. As best it can be determined, it falls between the *Installation and Operation* and *Maintenance* stages of the System Life Cycle overview as described in the Chief of Naval Operations (CNO) Information Assurance Publication 5239-16. Basically, this means that identification of vulnerabilities can be done by use of any of the following:

- System design documentation
- Certification Test and Evaluation results
- Site Test and Evaluation Results
- System security features
- Technical and procedural security controls
- System usage and audit reports
- Previous risk assessment documentation

Since no previous risk assessment documentation of the NPS network exists during the writing of this document, the NPS network has not yet been certified, and because access to much of the documentation of the NPS network has not been granted for this project, the majority of the vulnerability identification was done by interviewing

NPS personnel associated with the configuration and management of the network as well as comparing external vulnerability documentation of vendors with what the system characterization investigation revealed.

Since the .mil and .edu domains of the NPS network are essentially part of the same physical network, all vulnerabilities associated with either domain are present in both, because a network is only as secure as its weakest link. This is stated very clearly in the UTNProtect policy that has been laid out by the Navy and Marine Corps, and could be a potential problem when the .mil domain of the network needs to be certified for addition to the NMCI in the near future, but the consequences of this potential problem are beyond the scope of this paper.

B. GENERAL VULNERABILITIES

A preliminary investigation of the security posture of the NPS site revealed several site-specific vulnerabilities, which have been singled out and discussed below.

1. IA Staff

The most glaring vulnerability of the NPS network is a lack of staff devoted to the security of the network. As a result of not having sufficient staff, information assurance seems to be more of an afterthought than a daily consideration for the NPS network. With so few man-hours devoted to providing security to the network, the IA staff is only able to take care of the more pressing issues of the day, such as the latest virus threat, but isn’t truly able to keep ahead of the overall security posture of the network. As an example, security auditing is taking place on the NPS network, as necessary in any large network and a good practice to have in place, but the audit logs are not being given the review time needed to make them a useful part of the security plan.

Other issues like patch management are definitely a priority for the NPS network, but with so few on hand to propagate patches campus-wide, it is next to impossible for the staff to keep entirely up-to-date with the threats. With so many patches needed for newly discovered exploitable flaws, the time frame involved falls beyond an acceptable level of risk.

2. Training

Without continuous training on vulnerabilities and how to minimize them, another vulnerability, in essence, is being created. Most staff and users on the network have no security-specific training, which could be a potentially huge problem when it comes to user error and its consequences on security. This factor combined with the somewhat open atmosphere associated with any educational institution could be disastrous in the right circumstances. This is especially true considering that a percentage of the student population is being introduced to malicious exploits through coursework and could be responsible for accidental damage to the network. All Department of Defense facilities are supposed to have a training program in place to minimize the risk associated with user error, and since NPS falls under this category it should be no exception.

Another training issue that needs to be considered at NPS is the vulnerability that is created when staff members are relied upon to do their own software updates. Many staff members do not know how to do this properly and others think it is not important and do not worry about doing it at all. If staff members are being relied upon to update their own software, then they must have training to let them know the proper way to do updates. Training would also need to stress the importance of keeping software updated on a regular basis in order to minimize the vulnerabilities that exist on the system.

3. Configuration Management/Configuration Control Board

Although certain areas of campus are configured and updated regularly, there is no consistency to the process. Also, without proper training of staff as described above, many different versions of software are running on campus computers because they have not been properly updated. Adding to the problem is the fact that no centralized configuration management system or configuration control board exists on campus to make sure all systems at NPS are managed uniformly. These vulnerabilities can lead to serious security holes in the campus network.

The Information Assurance Vulnerability Alert (IAVA) process was designed by the Department of Defense to alleviate some problems sites were having with keeping configurations and patches current. By issuing IAVA alerts that must be acknowledged and complied with, they had hoped a certain level of security could be maintained among all DoD systems. NPS is one such site that must comply with IAVA alerts, but complying with the alerts simply means letting DISA know which systems have been updated via a web page that has been designed for this purpose. There is no penetration testing done by DISA to make sure sites are fully compliant, so even if a site is not keeping all systems updated according to the IAVA process, there is no way for DISA to know. NPS keeps as current as can be with the IAVA alerts, but when even they are not sure exactly what configurations they are dealing with at their own site, the IAVA process will not be much help in and of itself.

Being that NPS is an educational institution, strict enforcement of configurations is not always possible because of the academic nature of much of the work. Because of this, individuals are being allowed to administrate systems connected to the network without much knowledge of how to keep them secure, and are able to install software on machines without knowledge of IT staff. Although a certain amount of flexibility needs to be maintained at an educational institution to promote research and learning, this causes not only problems for that particular machine, but it may also open up security holes in the entire network.

Not having a centralized body responsible for decision-making also results in the situation of having a large amount of “rogue” servers on campus. These servers have been connected to the network for some reason or another that has probably been forgotten. As a result, no one among the IT staff is completely sure if these servers are still in use or what their purpose is, nor (in a lot of cases) even where they are located on campus. Not knowing much about what exists on the network and not knowing where machines are physically located so they can be disconnected from the network is an extremely vulnerable situation to be in, because if the security of these “rogue” servers is not being kept up, they are essentially an open door for attackers to enter the network.

4. Physical Security

NPS is a gated campus with guards posted at all entrances around the clock. This is a decent deterrent for outsiders who would like to enter campus for malicious reasons, although it is not entirely impossible to get access to the campus without credentials. People have successfully gained entrance to campus several times in the past, whether by sheer accident or by talking their way past the guards, and although these incidents have been benign, someone with less morality could gain admittance onto campus in the same manner if they were so inclined.

Unfortunately, the gated atmosphere of NPS also presents a false sense of security when it comes to securing the internal buildings of the campus. This leads to a less strenuous approach to physical security from those on campus responsible for the physical security of network devices and equipment associated with those devices. As a result of this false sense of security, many of the network devices that reside inside the gates of NPS have very lax physical security and could be easily accessed by anyone who really wanted to gain admittance to them.

This rather lax approach to physical security presents a very large vulnerability to the most common threat for all networks: the insider. Insiders are those people who are allowed access onto campus and have credentials that allow them that access. They are granted a certain level of trust, and with that trust comes a major vulnerability for the network if they have gained that it falsely. Because of the breakdown in physical security above and beyond the campus perimeter, a determined insider would have absolutely no trouble at all gaining access to physical devices connected to the network and installing malicious software or a network monitoring device. With a large portion of the student population being from foreign countries, and considering the constant variability of foreign policy, this could be a potentially serious vulnerability depending on the political climate of the time.

5. Proxy Server

NPS does not have a proxy server, making the site even more vulnerable to malicious software that can be downloaded from the Internet. A proxy server basically acts as a middleman between client machines and the outside world. If malicious software is being downloaded from a web page to a client machine, the proxy server can perform scans on the malicious software and may be able to detect it and destroy it before it infiltrates the network. If the proxy server is not able to destroy the malicious software before being infected itself, it is still able to contain any damage done before the internal network is exposed. Sometimes, this causes the proxy server to be become a sacrificial lamb of sorts for the network, but having to take down one server for repairs is preferable to having to cleanse an entire network of a virus infestation.

Without a proxy server present at NPS, client machines are able to download potentially malicious software directly from the Internet without a middleman to intervene. This could end up in an infection of the internal network without any possibility of containment. Combined with the lack of training of users of the network and lack of staff to clean up any infection on the network quickly, this could cause serious damage to data stored on the network and increased downtime for the entire network if infection were to occur., because it would result in a massive denial of service for the entire campus.

6. Backups

Many environmental threats that could possibly affect the NPS campus would have potentially devastating results in regards to the data stored on-site. The only way to recover from a catastrophic event like this is to have a contingency plan that includes backing up data and have a plan for restoring backups in the event the original data is lost. NPS does have a plan in place for backing up data, but one problem that could result in total data loss in the event that a catastrophic event occurred is not storing the backups properly.

NPS does weekly incremental backups of the most important data and full backups once a month, which is sufficient for recovery purposes if a small-scale disaster were to take and the backups were not affected by the disaster. The problem is that these backups are stored on-site and not stored in specially designed disaster-proof backup data storage units. This is not only a potential vulnerability if the entire site is ever affected by a catastrophic event, but also if the area where the backups are stored is affected by the event which results in the backups being destroyed. Any event that destroyed the on-site backups would result in loss of all the data with no possibility of recovery.

7. External Connections

An external connection to the Defense Management Data Center (DMDC) exists and is joined to the NPS campus network through a dedicated T-1 line that passes through the external router of the .mil domain. The DMDC is configured as a subnet on the NPS domain in order to have access to the mainframe for personnel data stored there. This is a backdoor to the network and presents a major vulnerability that could be exploited by just about anyone. The communication sent between the two sites is sent in the clear, so anyone with access to this T-1 line anywhere along its physical route would be able to tap in and steal or corrupt data being sent between the two. This also presents a major problem of an external source having trusted internal access to the NPS network if access can be gained through this backdoor.

C. SPECIFIC VULNERABILITIES

Although the previous vulnerabilities can definitely affect the security posture of a network, and should be treated seriously, the majority of exploits in a network are the result of hardware and software vulnerabilities. These vulnerabilities mainly exist because of the nature of the development process of most of the products used in any network environment, and are so easily exploited because they are shared with the hacker communities across the Internet. Since new vulnerabilities are being found daily and new patches are required to keep a system's security posture up-to-date, these vulnerabilities are often the toughest to guard against. This is further compounded by the fact that NPS does not have enough staff to realistically keep every system on campus patched completely, as was mentioned in the site-specific vulnerabilities above.

Since there are a lot of unknowns about the NPS network, it is nearly impossible to get a grasp, as a whole, on exactly which vulnerabilities are being guarded against and which are not, but a network is only as strong as its weakest link and any vulnerability at any point in the network causes a vulnerability for the entire network. By researching all hardware and software vulnerabilities associated with the configurations running on the NPS network, both .mil and .edu domains, a comprehensive list of possible vulnerabilities were identified and appear in the table of possible vulnerabilities in Appendix C. The table also contains the estimated likelihood of exploitation of the vulnerability, the magnitude of impact if exploitation were to occur, and an assigned level of risk for the vulnerability.

THIS PAGE INTENTIONALLY LEFT BLANK

V. COUNTERMEASURE RECOMMENDATIONS

A. OVERVIEW

In the previous chapter, the vulnerabilities were identified and the risk associated with those vulnerabilities was determined. This chapter attempts to eliminate, or at the very least mitigate, as much of the identified risk as possible by suggesting countermeasures that can be applied. By eliminating or mitigating the risk associated with the network's vulnerabilities, the residual risk of the system and its data should be able to be brought within an acceptable level during the certification and accreditation process. Keeping in mind that no organization has limitless resources for placing countermeasures on their network, the suggested countermeasures are as cost-effective and practical for the NPS environment as possible. Each suggested countermeasure is discussed in detail below.

B. RECOMMENDATIONS

1. Auditing

Auditing is easily one of the least utilized countermeasures in all of network security at NPS, but it is also one of the most important if administrators are to be proactive in the hardening of their network. Minimal auditing is taking place at NPS, and that is an important start, but the audit logs are not being reviewed on a regular basis and this can be potentially dangerous. Sometimes audit logs are the only thing that can be relied upon when all other lines of defense are showing that nothing is wrong in a network.

Auditing events that may point to potential attacks on a network may give network administrators a chance to catch an attacker before an attack actually happens. The only way this could be a success, though, is if someone is analyzing the audit logs for those scenarios on a regular basis. If attack scenarios are spotted early on, steps can be taken to make sure no further damage is done. This is why audit logs are such an important part of any network security plan.

Audit logs are also one of the few ways administrators will be able to deter or catch any malicious insiders that may be abusing their privileges. Knowing that their actions are being audited is a major deterrent for most users of a system, but for the small percentage that is not deterred by this knowledge, auditing and reviewing audit logs is a sure way to catch them red-handed. To ensure that the malicious insiders are not able to tamper with the audit logs as well to cover their tracks, a separation of duties system should be put into place.

Most networks have multiple administrators all with the same privileges, which allows anyone who maliciously gains access to one of those accounts full administrator privileges and free reign to do whatever damage they want to the network. If each administrator account were restricted to only the access needed for the person to do their assigned duties, (i.e. one person handles audit logs, one person handles opening new accounts, etc.) multiple people would need to collaborate in order to both commit malicious activities and cover it up by editing or deleting the audit logs. Since everyone goes through a background check at NPS, the odds of one malicious insider getting another insider to help with malicious activities are very slim and will probably result in someone in authority being told. This separation of duties in regards to audit logs is vital if malicious insiders are to be caught.

Another step in the importance of auditing is the analysis of audit logs. Analyzing audit logs is no easy task, though, and requires a great amount of training for any individual chosen to perform this particular duty. Volumes of knowledge must be learned about how attackers carry out their malicious tasks, in order to be able to spot the telltale signs of an attack as it is taking place. If the person analyzing the logs does not know what to look for, the audit logs are not serving their intended purpose, and the security of the network suffers.

Audit logs are also important in the event that it is known an attack has occurred and administrators of the network are not sure how or when it was committed. This is where audit logs come in. Audit logs can be an important asset in any forensic investigation of a break-in, because they answer the how and when of attacks that have taken place and allow for patching of security holes that may have been overlooked.

Because of the importance of the audit logs and their use in retracing the steps of attackers, they cannot be stored where an attacker would be able to destroy or edit them. They can be stored in a remote location or in several locations at once to ensure redundancy, but in either case, they should be reviewed regularly and backed up in case a question about a possible attack arises later. Backups of the audit logs should be secured from anyone other than those who have access to the original audit logs, otherwise there is a chance that the audit logs could fall into the wrong hands.

2. Increased Security Personnel

Many of the problems with the security of the network at NPS stem from the fact that there is not enough personnel dedicated to the protection of the network. All other countermeasure recommendations are based on this one, because more cannot be done without an increase in the security personnel available. Without having sufficient personnel to carry out tasks vital to the security of the network, they simply do not get done properly or sometimes at all. The current security personnel do the best they can with the resources they have available to them, but this is not enough to secure the NPS network.

More personnel are needed when it comes to things such as rolling out critical updates campus-wide when new malicious software has been detected and a new patch has been released. Usually by the time a patch has been released, malicious software is already spreading across the Internet, so timing is essential. Installing patches as quickly as possible to all campus machines is a necessary step in the protection of the network because it seals a previously unknown hole in the network's defenses before it can be exploited by attackers. The sooner steps like these are taken, the better off the security posture of the network is, and without enough personnel to carry out patching, the longer the security hole remains open.

Increases in personnel would also be vital if audit logs are going to be a useful part of the defense of the network. Although auditing is being carried out at NPS, much auditing that could be done is not being done because there just is not anyone to review the logs on a regular basis. When logs are being kept but not being reviewed, they really do not serve much purpose for the security of the network, except as an afterthought to confirm that there was an attack and how it was carried out. Increasing personnel would enable audit logs to be reviewed daily and could result in detection and prevention of malicious activity before it could cause any major damage.

3. Training

Training personnel who manage or use a network is critical in the protection of systems connected to the network. If users are not properly trained on what they should or should not be doing on a network, user error creates a major vulnerability to the network. Personnel managing the network should be trained in general information assurance practices as well as trained to use specific software/hardware associated with the NPS network. This includes, but is not limited to, routers, intrusion detection systems, firewalls, servers, network scanning tools, operating systems used at the site, and any software running on those operating systems. While no one person can be an expert in every single area of a large network like NPS, the combined knowledge of the network management team should be as complete as possible as it pertains to the network.

Much of the general information assurance knowledge can be learned from coursework here at the university or from graduate students here who have taken those courses and are looking for a place to put that knowledge to work. A university that prides itself on having one of the best computer science security curricula in the country should have a network that reflects that distinction, and the resources to make it a reality are definitely available. A program that creates a relationship between the security track curriculum and the network security personnel at NPS might be a beneficial venture all around.

As far as the specific training needed for hardware and software being used on campus, outside sources will most likely be needed. Given that NPS is situated near what many consider to be the technology epicenter of the world, Silicon Valley, outside sources should not be tough to acquire. Many of the manufacturers of the hardware and software that NPS uses are located in the Silicon Valley area and give seminars about their products on a regular basis. Some of these manufacturers have even come to NPS to give talks recently and would probably be more than happy to do so again. If the administrators of the network at NPS could take advantage of these resources, much could be learned about the vulnerabilities of the products used on the network and how those vulnerabilities could be mitigated.

With a network management team that is well-versed in keeping the network secure, passing this knowledge on to the users of the systems at NPS would be a very simple process. All incoming staff and students could be given network security training as a predecessor to being given an account with which to log on to the campus network. This training would be rather basic, but comprehensive enough to minimize user error and keep systems from being victims of ignorance. Subjects such as choosing good passwords, opening email attachments, and activating modems for unauthorized dial-in usage could be covered, as well as any other topics deemed necessary. Of course, this would not completely eradicate the problems, but at least misunderstanding of the consequences of these actions would be diminished and the NPS community as a whole would be more aware of their role in the security of the network.

4. Configuration Management

Good configuration management is a key ingredient in any large system if that system is to be secure. Having good configuration management would give the administrators of the NPS network a better idea of what exists on their systems and where those systems are located. Having a centralized entity that is responsible for making sure all systems on campus are enforcing the security policies would increase the security of the network immensely. This centralization process could be accomplished by creating a configuration control board to make configuration decisions or by investing in configuration control software to carry out configuration tasks, although the best solution would be a combination of these two approaches.

A configuration control board would be a great idea for NPS so that decisions on how the network should be configured could be discussed among key personnel and decided on accordingly. Having a committee to make these decisions would allow for more control over what was to be used and where it was to reside and would make sure that no individual was making these decisions without knowledge of those in charge. General campus configurations of hardware such as routers, firewalls, and servers would be more secure if they were decided upon by a group of people educated in the language of these devices, rather than decided on by individuals who may not be qualified. Also, by investigating what software and services are truly needed by the campus community and basing configuration decisions on the results, excess security holes could be lessened as much as possible and the principle of least privilege could be maintained.

As an addition to the decision-making process of the configuration control board, configuration management software could be used to enforce the policies set forth by those decisions. There are many configuration management software solutions available, and by investing in one of these, NPS network administrators could make sure all machines on campus are running a pre-defined set of configurations based upon the policies created by the configuration control board. Configuration management software would provide a level of consistency that is lacking on the NPS network by making sure security settings on all devices are the same and enforce security policy. It would also ensure a higher level of proactive enforcement of security policies and allow NPS personnel to maintain more control.

5. Physical Security

Although physical security is already in place at NPS in the form of the perimeter gate guards, this doesn't necessarily mean that physical security is not a countermeasure that needs to be further refined. Physical security of all devices connected to the network, especially the backbone of the network, needs to be a priority. If someone has physical access to a device, the device can be completely controlled by them, which would mean they would be able to bypass any other security mechanisms that may be in place. This situation must be taken seriously and prevented at all costs or else the rest of the security that has been put in place on the network is all for naught.

Many exterior doors at NPS are left unlocked in the evenings after everyone has left for the day, which allows indoor access to buildings containing network devices. Also, many network devices are kept in rooms with cipher locks to which more people than necessary know the combination. Since need-to-know policies are not being strictly enforced, some of these people who have the combinations do not need them, and should therefore not know them. Even if the combination is not known, though, it has been proven that the 5-key cipher locks used on campus are not incredibly difficult to crack by brute force in a relatively short period of time. Given access to these doors when no one else is around (i.e., in the evenings), anyone would be able to gain entrance to a locked room containing network devices. An attacker would then be able to do any one of a number of malicious things, all of which would result in decreased security posture of the network and possible loss of data confidentiality or integrity.

To protect physical access better to rooms containing network devices, doors should be protected with 10-digit keypads with authorization codes of at least eight digits, and possibly magnetic card strip readers in locations containing backbone devices for the network. Access to these rooms should be granted only to personnel who need to have access on a daily basis and the authorization codes should not be given to anyone else unless they undergo an authorization process controlled by management. Closed-circuit hidden cameras should be used to monitor the entrances to these secure rooms, or at the very least installation of fake cameras that are highly visible can be used to deter break-ins.

6. Proxy Server

Installation of a proxy server is another line of defense that could be used to secure the NPS network. A proxy server acts as a middleman between the Internet and client machines on the NPS network by sending client requests and receiving replies from web servers. Requests for web resources always pass through the proxy server and responses to those requests can be checked for malicious software before being sent along to the client that requested the resource.

Currently, NPS relies completely on the antivirus software it has installed on client machines across campus to stop malicious software infections. Although antivirus software is a necessary part of any defense-in-depth approach to network security, relying solely on antivirus software is not enough. When malicious software is downloaded to a client with antivirus software, it becomes a race between the antivirus software detecting and the malicious software infecting. This is a battle that the malicious software will, more than likely, win, especially if the antivirus signatures are not regularly updated.

Taking the chance that antivirus software won't be able to quarantine malicious software before it infects the network is not a chance any secure network's administrator should take.

By installing a proxy server, NPS would have a first line of defense against malicious software being downloaded from the Internet, and could potentially stop and quarantine any malicious software that was detected. A proxy server also caches many web resources that are used most often by NPS personnel, so that fewer downloads are necessary and contact with the virus-infested Internet is minimized.

7. Patch Management

Patch management is probably one of the most important jobs of any network security personnel, because of the inherent flaws in the software development process that are carried down into the commercial products used in all networks, including the NPS network. New flaws are constantly being discovered in systems that are in place in a network, which means new patches are constantly being developed to combat those flaws. If these patches are not installed on systems that contain the flaws in a relatively short time frame, attackers are free to exploit those flaws and gain access to unprotected networks.

Since there is a lack of sufficient personnel to carry out adequate patch management at NPS, as discussed above, patches needed to close holes in the security of the network often do not get the attention they deserve. By scanning the network for well-known exploits, which is actually done on a regular basis, it is easy to see that NPS is not completely up-to-date on its patch management. The same vulnerabilities are sometimes discovered week after week because they have not yet been patched. Although getting rid of all vulnerabilities in a network is an impossible task, installing readily available patches to fix well-known security holes in a network must be done and is one of the first things any network administrator should do to begin securing their network. A vast majority of the vulnerabilities listed in the previous chapter are exploits that could be easily prevented by installing an available patch. A good patch management plan would go a long way to fixing this particular issue.

A patch management plan goes hand in hand with a configuration management plan, and should be implemented at the same time for simplicity. If the configurations on network computers are standard, testing patches on several representative machines becomes possible and rolling out the patches across all machines becomes a much simpler and faster process. By refining the entire process of patching, administrators can achieve a more proactive approach to defending the network instead of always trying to clean up a disaster that has already occurred. Many patch management software solutions are also available that could be used to make sure all machines are up-to-date with their patching needs as easily as possible.

8. Backups

NPS does weekly incremental backups and a full backup every month in order to protect themselves from data loss in the event of a catastrophic event, but those backups are stored on-site and not well protected. These backups should be stored in disaster-proof backup data storage units at the very least to protect from any minor incidents on campus. These storage units protect backup tapes from melting in the event of a fire or from destruction by water in the event the sprinkler systems are activated or a flood occurs. This will ensure recovery of data if a minor disaster occurs and affects some, but not all, of the campus environment

Ideally, though, NPS needs to store their backup tapes redundantly at an offsite facility in case of a disaster that affects the entire site. If a disaster destroys the backups that are stored on site as well as the original data, NPS would have no way of recovering and restoring data and everything would be lost. If backups, however, are stored in an off-site facility that is in another location, the chances of the disaster striking both places simultaneously are very minimal, so full recovery and restoring of data would still be quite possible in an emergency situation.

9. External Connections

Any external connection to a network should be considered a potential point of attack no matter how insignificant it may appear. The external connection that comes into the NPS network from DMDC at Fort Ord should have more security associated with it if it is to be considered safe from attack. Even though the Fort Ord facility is trusted, and physical access to that facility is not a realistic attack strategy, attackers are still able to gain physical access to the T-1 line itself if they know this connection exists.

At the very least, the data being sent back and forth between the two sites should use strong encryption in the event that a man-in-the-middle attack takes place. This would prevent any data that was gained from being read in the clear and prevent attackers from using replay attacks. NPS should also practice the principal of least privilege by only allowing admittance to areas of the network that need to be accessed from this connection instead of allowing access to the mainframe. If a malicious attacker was able to gain entry to NPS from this backdoor, they should not be able to have free reign. If everyone connecting to NPS through this connection is subject to security procedures that verify their identity and limit their activity, severity of an attack from this connection could be lessened measurably.

VI. CONCLUSION

Certification and accreditation is a set of rigorous procedures defined in Department of Defense Instruction (DoDI) 5200.40, and a requirement of any system that is being operated or developed by the Department of Defense. Since the Department of the Navy oversees the Naval Postgraduate School, it falls under the jurisdiction of the Department of Defense, and as a result, must follow the guidelines set forth by the DoD. As a result of these guidelines, the Naval Postgraduate School's gigabit network must undergo the certification and accreditation process. A current effort is underway at the time of writing, to conduct certification and accreditation procedures on the NPS gigabit network. The purpose of this paper is to assist in the certification process of the NPS network by conducting a thorough risk assessment of the network and reporting the results, which can in turn be used to help make the decision whether or not the network should be certified and accredited.

At the beginning of the investigation of the NPS network, there were a lot of questions to ask, some of which turned out to be easy and others of which turned out to be more difficult, but all of which needed to be answered if a thorough risk assessment was to be conducted. Many of the initial questions involved the physical layout of the network, which was able to be determined in the first stage of the risk assessment process: system characterization. System characterization is conducted as a first step to the risk assessment process in order to determine the scale of the network and where the accreditation boundary lies, the hardware and software involved, and the external connections of the network. This stage of the risk assessment process consisted mostly of viewing existing diagrams of the network, scanning the network to corroborate what was shown in the diagrams, and physically inspecting the network devices and their connections. In the end, a comprehensive view of the layout of the network and its connections was established. Once the questions about the physical layout of the network were answered and the picture was completely understood, the next stage of the risk assessment process could begin.

The second stage of the risk assessment process, threat identification, involved taking stock of the environment surrounding the NPS gigabit network and determining what threats could be found in that environment. Many threats are somewhat generic which makes them the same for all networks, and the NPS network is no exception. Insiders, outsiders, and environmental threats can relate to any system, but how these threats relate to the NPS campus specifically needed to be determined during phase two. Determining the depth of the insider and outsider threats was a somewhat difficult concept, but environmental threats were a little more concrete. Investigation of these threats not only gave an understanding of how the network might be penetrated, but it also allowed a greater understanding of what sorts of countermeasures would later need to be put into place to combat these threats. After threats were identified, identification of the vulnerabilities was the next step taken in the risk assessment procedure.

Stage three of the risk assessment further allowed for development of countermeasures by investigating what vulnerabilities exist in the NPS environment. This step, along with the previous one, are the key elements in determining what risks are affecting the system. Vulnerability identification involved going back to the system characterization to investigate what possible vulnerabilities could exist given the configuration of the network and then determining whether those vulnerabilities were present. Investigating the security procedures for the network, such as patching, auditing, and configuration management, during this stage gave a complete picture of what vulnerabilities could be expected and made narrowing down the list of possible vulnerabilities an easier task. Of course, after the investigation was finished, patching and changes in the network continued to take place, because the NPS network is a system in use on a daily basis. This may have resulted in the list of vulnerabilities changing, but these are things that need to be dealt with when performing a risk assessment on a changing network.

Determining every conceivable vulnerability is most likely not a possibility for any network this size, but by collecting as much information as possible during this stage of the risk assessment process, the network is much more secure when the countermeasures have been determined and applied. Also, the more work that is put into finding vulnerabilities at this stage, the more informed the DAA can be in making the decision whether or not to certify and accredit the system. No system is completely without vulnerabilities, but the DAA cannot make an informed decision if he doesn't have the most thorough information available.

After characterizing the system, identifying the risk, and identifying the vulnerabilities of the network, risk analysis was able to be performed and countermeasures were then able to be suggested. Analysis of the risk was done by assessing the likelihood of successful exploitation of a vulnerability, the magnitude of impact if a vulnerability were to be exploited, and then assigning each vulnerability a level of risk. Overall, it was found that the risk associated with the vulnerabilities found was medium to high, which suggests that countermeasures needed to be put in place to lower the risk to an acceptable level if the network were to be successfully certified and accredited.

Suggested countermeasures were decided upon according to how much they would impact the NPS gigabit network's security posture without being afforded an unlimited budget. Some countermeasures that were suggested were conducting better configuration management, patching more rigorously, and reviewing audit logs on a regular basis, among others. These countermeasures are by no means out of reach of the current network administration, and should be implemented even without the certification and accreditation process taking place. For the most part, the only suggested countermeasure that has budgetary concerns attached to it is the suggestion that more security personnel be hired to help implement all of the other countermeasures. This may be the most important suggestion, though, because of the already existing lack of qualified personnel and the extra workload suggested by adoption of these countermeasures. By adopting the countermeasures that have been suggested, a heightened level of network security can be realized, and should be an effective tool for getting the NPS network certified and accredited by the DAA. Even so, by no means is it suggested that the level of risk will be lowered to nil.

The risk assessment of any network that is already in use, such as the Naval Postgraduate School's gigabit network during the writing of this document, is a changing and constantly evolving process. As such, the architecture, configuration, and security posture of the network is most likely not exactly the same at the conclusion of this investigation as it was when the investigation was begun, but every effort has been made to consider the future of the network and how it will affect the risk assessment process. To further complicate matters, the NPS network is currently undergoing some changes as it splits into the .mil and .edu domains, but the overall threats, vulnerabilities, and risks will remain constant, which makes the recommended countermeasures all the more important as these changes are being made.

NPS is a somewhat unique network in the DoD in that it is connected with a university atmosphere on one side and a military atmosphere on the other. The university community is notorious for having lax security and is much of the reason behind the security posture of the entire Internet to this day. The military community on the other hand is constantly trying to improve the security posture of their networks to keep intruders out. The NPS network falls in the unexplored gap between the two. Security is a concern, but not as much of a concern as most military installations, because of the less critical nature of the information stored within. Being that the overall criticality of the system at NPS is low, some of the risk associated with the vulnerabilities present is acceptable. Overall, though, it was determined that there is improvement needed as it applies to the security posture of the network. If the suggested countermeasures are put in place, there should be no problems with certifying or accrediting the system.

APPENDIX A. SERVER LIST

Name	OS	Dept	Domain	Description	Admin
CASTOR	Microsoft Windows NT Server 4.0	ACS	NPGS	Autocad server	
MERCY	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Backup and restores	Eldor Magat
HAMPTON	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Citrix	Charles Taylor
HOUSTON	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Citrix	Charles Taylor
Ducktail	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Citrix Servers	Charles Taylor
Flatop	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Citrix Servers	Charles Taylor
Mohawk	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Citrix Servers	Charles Taylor
Weave	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Citrix Servers	Charles Taylor
PITA	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Citrix Travel Manager	Charles Taylor
DMS	Microsoft Windows 2000 Server	EWS	NPGS	Defense Messaging Server	Rhoda Lynch
Growler	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Domain Controllers	Eldor Magat
Intrepid	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Domain Controllers	Eldor Magat
Midway	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Domain Controllers	Eldor Magat
Thorn	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Domain Controllers	Eldor Magat
IT003606	Microsoft Windows 2000 Advanced Server	Contractor	NPGS	DORS Development	David Wang
PTCRUISER	Microsoft Windows 2000 Advanced Server	Contractor	NPGS	DORS Development	David Wang

Name	OS	Dept	Domain	Description	Admin
FIBER	Microsoft Windows 2000 Advanced Server	EWS	NPGS	EHF	Neil Harvey
PDC-51TRAIN	Microsoft Windows 2000 Advanced Server	EWS	EWS	EWS Test	Eldor Magat
AMERICA	Windows 2000 Advanced Server	EWS	NPGS	Exchange Servers	Renee Lightcap
Ellis	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Exchange Servers	Renee Lightcap
Elrod	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Exchange Servers	Renee Lightcap
Essex	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Exchange Servers	Renee Lightcap
Grasp	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Exchange Servers	Renee Lightcap
Pecos	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Exchange Servers	Renee Lightcap
Saipan	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Exchange Servers	Renee Lightcap
EXCHANGE1	Microsoft Windows 2000 Server		EWS	Exchange test server	Renee Lightcap
Raven	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Fastdata	Bob Sharp
RAMAGE	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Fastdata Test Server	Bob Sharp
Triton	Windows 2000 Advanced Server		NPGS	File server	Eldor Magat
DELMONTE	Microsoft Windows NT Server 4.0	EWS	NPGS	File Server ETAC	Mike Nichols
Cyclone	Microsoft Windows 2000 Server	EWS	NPGS	File servers	Eldor Magat
Falcon	Microsoft Windows 2000 Advanced Server	EWS	NPGS	File servers	Eldor Magat
Kiska	Microsoft Windows 2000 Advanced Server	EWS	NPGS	File servers	Eldor Magat
Nimitz	Microsoft Windows 2000 Advanced Server	EWS	NPGS	File servers	Eldor Magat

Name	OS	Dept	Domain	Description	Admin
RUSHMORE	Microsoft Windows NT Server 4.0	EWS	NPGS	File servers	Eldor Magat
Yukon	Microsoft Windows 2000 Advanced Server	EWS	NPGS	File servers	Eldor Magat
GOLF1	Microsoft Windows 2000 Server	EWS	NPGS	Financial/Accounting	Golf Course
LEXINGTON	Microsoft Windows NT Advanced Server	EWS	NPGS	Gone	Eldor Magat
AZTEC	Windows 2000 Advanced Server		NPGS	Landesk Server	Bob Sharp
INCA	Windows 2000 Advanced Server		NPGS	Landesk SQL 2000	Alan Pires
eagle	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Landesk Test server	Bob Sharp
Max	Microsoft Windows NT Server 4.0	EWS	NPGS	Maximo	Bob Sharp
UPDATER	Microsoft Windows 2000 Advanced Server	EWS	NPGS	MS windows Updater	Greg Pierson
NAS02B	Microsoft Windows 2000 Server	EWS	NPGS	NAS File Servers	Mike Nichols
NASCCMR1	Microsoft Windows 2000 Advanced Server	EWS	NPGS	NAS File Servers	Mike Nichols
NASSAU	Microsoft Windows 2000 Advanced Server	EWS	NPGS	NAS File Servers	Eldor Magat
STRINGRAY	Unix	EWS	NPGS	NAS File Servers	Eldor Magat
TORNADO	Unix	EWS		NAS File Servers	Eldor Magat
Copperhead	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Norton Antivirus	Charles Taylor
Krait	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Norton Antivirus	Charles Taylor
Mamba	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Norton Antivirus	Charles Taylor
MAYAN	Windows 2000 Advanced Server	EWS	NPGS	Not assigned yet	Eldor Magat
OCL2	Microsoft Windows NT		OAPIW	OAPIWEB	

Name	OS	Dept	Domain	Description	Admin
	Server 4.0		EB		
IT003477	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Python Web Management	Stacy Laabs
GREYFIN	Microsoft Windows NT Server 4.0	NOC	NPGS	RAS	Lonna Sherwin
LAFAYETTE	Microsoft Windows 2000 Advanced Server	Special Projects	NPGS	Remedy Server	Alan Pires
DIANA	Unix/Linux		NPGS	Samba	
ERIS	Unix/Linux		NPGS	Samba	
MISSAS	Microsoft Windows 2000 Server	EWS	NPGS	SAS Server	David Wang
OTTER	Microsoft Windows 2000 Advanced Server	EWS	NPGS	SMS Server	Bob Sharp
CAPABLE	Microsoft Windows 2000 Advanced Server	Special Projects	NPGS	SQL	Alan Pires
MC01BDB	Microsoft Windows 2000 Advanced Server	Special Projects	NPGS	SQL 2000	Alan Pires
sunfish	Microsoft Windows 2000 Advanced Server	Special Projects	NPGS	SQL Development	Alan Pires
Bullnose	Microsoft Windows 2000 Server		NPSEXTRA	Web Servers	Charles Taylor
Seawolf	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Web Servers	Chris Abila
RANGER	Microsoft Windows 2000 Advanced Server	EWS	NPGS	Web Testing	Chris Abila
FIFE	Microsoft Windows NT Server 4.0	EWS	NPGS	WINS	Eldor Magat
ACSAPPS	Microsoft Windows 2000 Advanced Server	ACS	NPGS		
AIRBORNE	Microsoft Windows 2000 Advanced Server		MOVES		
ATLANTIS	Unix		NPGS		
AUTONOMY	Microsoft Windows 2000 Advanced Server		NPGS		
BARNEY	Microsoft Windows 2000 Server		NPGS		Debbie Kreider

Name	OS	Dept	Domain	Description	Admin
BEEHIVE	Windows 2000 Advanced Server				
BOA	Microsoft Windows 2000 Advanced Server		NPGS		
BOXER	Microsoft Windows 2000 Advanced Server		NPGS		
BRINK01	Microsoft Windows 2000 Server		NPGS		
CASCADE	Microsoft Windows 2000 Server		NPGS		
CEESERVER	Microsoft Windows 2000 Server		NPGS		
CHIMERA	Windows 2000 Server				
COLE	Windows 2000 Advanced Server				
CYPRESS	Microsoft Windows 2000 Server		SAAM		
D68RWX11	Microsoft Windows 2000 Server				
DLRC_SERVER	Microsoft Windows 2000 Advanced Server	DLRC	NPGS		
DLRC-SERVER2	Microsoft Windows 2000 Advanced Server	DLRC	NPGS		
DRCAFENT	Microsoft Windows NT Server 4.0		DRCAF EWG		
DRMI135	Microsoft Windows 2000 Server	DRMI	NPGS		Steve Hurst
DRMI159	Unix	DRMI			Steve Hurst
DRMIMAIN	Microsoft Windows 2000 Server	DRMI	NPGS		Steve Hurst
DRMISQL	Windows 2000 Advanced Server				Steve Hurst
ELO					
ESLLAB	Windows 2000 Server		NPGS		Greg Pierson
EUROPA	Microsoft Windows 2000		NPGS		

Name	OS	Dept	Domain	Description	Admin
	Server				
EVANGELION	Microsoft Windows 2000 Server		NPGS		
EXEC1	Microsoft Windows 2000 Advanced Server	File	NPGS		Eldor Magat
EXEC2	Microsoft Windows 2000 Advanced Server	Exchange	NPGS		Eldor Magat
GL-ADMIN	Microsoft Windows 2000 Advanced Server		NPGS		
IAGO	Microsoft Windows 2000 Server		MOVES		
IJWA	Microsoft Windows 2000 Server		NPGS		
IJWAS01	Windows 2000 Server				
IS~RANGER	Microsoft Windows 2000 Server		NPGS		
IT003584	Microsoft Windows 2000 Server		WORKGROUP		
ITAPSSERVER			NPGS		
KNOX-LIBRARY---	Microsoft Windows 2000 Server	KNOX LIBRARY	WORKGROUP		KNOX LIBRARY
KNXSPT	Windows 2003 Server Enterprise Edition				KNOX LIBRARY
knxsql	Microsoft Windows 2000 Advanced Server	KNOX LIBRARY	NPGS		KNOX LIBRARY
KNXUP1	Windows 2003 Server Enterprise Edition				KNOX LIBRARY
KNXUP2	Windows 2003 Server Enterprise Edition				KNOX LIBRARY
KNXWWW	Microsoft Windows 2000 Advanced Server	KNOX LIBRARY	NPGS		KNOX LIBRARY
libra	Unix				
LRCAPPS	Microsoft Windows 2000 Advanced Server	ACS	NPGS		
M058802	Microsoft Windows 2000 Server		NPGS		

Name	OS	Dept	Domain	Description	Admin
M076699	Microsoft Windows 2000 Server		NPGS		
MAGOG	Microsoft Windows 2000 Advanced Server		NPGS		
MARINES	Microsoft Windows NT Server 4.0		NPGS		
MARLIN	Microsoft Windows 2000 Server		MARLIN-WG		
MC01BAPP	Microsoft Windows 2000 Advanced Server	Special Projects			Alan Pires
MC01BEMS	Microsoft Windows 2000 Advanced Server	Special Projects			Alan Pires
METRICSSRV	Microsoft Windows 2000 Advanced Server		METRICS		
MIAMI	Windows 2000 Advanced Server				Charles Taylor
MONITOR	Microsoft Windows 2000 Server		NPGS		
MOTHRA	Microsoft Windows 2000 Advanced Server		NPGS		
NETPLOT	Microsoft Windows NT Server 4.0		NPGS		
NHSERVER	Microsoft Windows 2000 Server		NPGS		
NPSUPDATER	Microsoft Windows 2000 Advanced Server	EWS	NPGS		Greg Pierson
ORION	Microsoft Windows 2000 Server				
PEACH	Microsoft Windows 2000 Server		SAAM		
Penguin	UNIX				Eldor Magat
RAVEN	Windows 2000 Advanced Server				Bob Sharp
REPUBLIC	Windows 2003 Server Enterprise Edition				
Scorpion	NAS Box				Homeland

Name	OS	Dept	Domain	Description	Admin
SCOTTY	Microsoft Windows 2000 Advanced Server		NPGS		
SEABEEONE	Microsoft Windows 2000 Advanced Server		NPGS		
SP433LAB22	Unix				
SRVSA22	Microsoft Windows 2000 Server		NPGS		
TERRA	Microsoft Windows 2000 Server				
TURTLE4	Microsoft Windows 2000 Advanced Server		SECAPS		
W2KSVR-I380	Microsoft Windows 2000 Server				

APPENDIX B. BASELINE FIREWALL SETTINGS

No.	Service	Port	Protocol	Policy		Conditions		Comments
				In	Out	In	Out	
1.	Blackberry	3101	TCP	Denied	Cond.	Denied	1. Handheld device must utilize S/MIME. 2. Must be server-side and client-side SSL enabled for authentication using DoD PKI. 3. Encryption must use FIPS-compliant algorithms for Sensitive Information. 4. At a minimum, the Handheld Device must be connected to the Blackberry MS Exchange Enterprise Server Version 2.1 Service Pack 3 or greater and have desktop version 5.16 or greater.	
2.	CITRIX	1494	TCP	Denied	Cond.	Denied	1. Must use CITRIX ICA Thin Client. 2. Must use 128-bit encryption. 3. Must use IP filtering. 4. Shadowing disabled.	
3.	DISA SWA*	9023	TCP	Denied	Cond.	Denied	1. Must be SSL enabled. 2. Encryption must use FIPS-compliant algorithms for Sensitive Information.	* SWA = Secure Web Access

No.	Service	Port	Protocol	Policy		Conditions		Comments
				In	Out	In	Out	
4.	DISA SWA*	9024	TCP	Denied	Cond.	Denied	1. Must be SSL enabled. 2. Encryption must use FIPS-compliant algorithms for Sensitive Information.	* SWA = Secure Web Access
5.	DISA SWA*	9025	TCP	Denied	Cond.	Denied	1. Must be SSL enabled. 2. Encryption must use FIPS-compliant algorithms for Sensitive Information.	* SWA = Secure Web Access
6.	DISA SWA*	9026	TCP	Denied	Cond.	Denied	1. Must be SSL enabled. 2. Encryption must use FIPS-compliant algorithms for Sensitive Information.	* SWA = Secure Web Access
7.	DNS	53	UDP, TCP	Denied	Cond.	Denied	1. Permitted through firewall via a split DNS architecture.	1. Inbound DNS queries to be handled by external server in split DNS configuration. No inbound external queries to be passed through firewall.
8.	FTP	20, 21	TCP	Denied	Cond.	Denied	1. Application proxy required if available.	
9.	FTPS	989, 990	TCP	Cond.	Cond.	1. Must be SSL enabled. 2. Minimum authentication requirement is utilization of SSL's inherent user ID and password capability. Client authentication must be done using DoD PKI certificates. 3. Must use IP filtering to host IP address. 4. Not permitted for use with Sensitive Information.	1. Must be SSL enabled. 2. Not permitted for use with Sensitive Information.	1. Use of FTPS for Sensitive Information PROHIBITED until FIPS compliant cryptographic module becomes available.

No.	Service	Port	Protocol	Policy		Conditions		Comments
				In	Out	In	Out	
10.	HTTP	80	TCP	Denied	Cond.	Denied	1. Application proxy required.	1. A filter may be integrated to prevent the accessing of objectionable sites and select MIME types. 2. Information intended to be publicly available should be placed on a public HTTP server on the outside of the firewall.
11.	HTTPS	443	TCP	Cond.	Cond.	1. Only to authorized servers with DoD PKI server certs from authenticated users. 2. Minimum authentication requirement is utilization of SSL's inherent user ID and password capability. When available, client authentication must be done using DoD PKI certificates. 3.Must use IP filtering to host IP address. 4. Encryption must use FIPS-compliant algorithms for Sensitive Information.	1. Application proxy required.	1. Information intended to be publicly available should be placed in the DMZ/Service Network.
12.	IMAPS	993	TCP	Cond.	Cond.	1. Certificate verification through DoD PKI certificate authority. 2. Restricted by source and destination IP.	1. Destination IP restricted.	

No.	Service	Port	Protocol	Policy		Conditions		Comments
				In	Out	In	Out	
13.	ISAKMP	500	UDP IP 50 IP 51	Cond.	Cond.	1. Authorized ONLY if VPN meets conditions of Para 6.2.3 or 6.2.4 of UTNProtect Policy. 2. Source/Destination IP filtering required.	1. Authorized ONLY if VPN meets conditions of Para 6.2.3 or 6.2.4 of UTNProtect Policy. 2. Source/Destination IP filtering required.	1. CNO / CNNWC approval is required, prior to configuration/use, of VPNs that DO NOT meet the conditions of para 6.2.3 or 6.2.4 of the UTNProtect Policy. See Section 6 (paras 6.3.1 and 6.3.2) for further information.
14.	LDAP	389	TCP	Cond.	Cond.	1. Restricted by source and destination IP. 2. Requires CNO/CNNWC approval. Contact CNO N61C4 / CNNWC, or PMW 161 POC for further information.	1. Restricted by source and destination IP.	
15.	LDAPS	636	TCP	Cond.	Cond.	1. Restricted by source and destination IP. 2. Certificate verification through DoD PKI certificate authority.	1. Restricted by source and destination IP.	
16.	Lotus Notes	1352	TCP	Cond.	Cond.	1. Use restricted by server source and destination IP.	1. Use restricted by server source and destination IP.	
17.	NES	N/A	IP 055, IP 029	Cond.	Cond.	1. Usage restricted by NES to NES source and destination IP.	1. Usage restricted by NES to NES source and destination IP.	
18.	NNTP	119	TCP	Denied	Cond.	Denied	1. Outbound NNTP requests are proxied through the firewall to external servers. 2. Usage restricted by server-to-server source and destination IP.	1. A filter may be integrated to prevent accessing of objectionable newsgroups or content.

No.	Service	Port	Protocol	Policy		Conditions		Comments
				In	Out	In	Out	
19.	NNTPS	563	TCP	Denied	Cond.	Denied	1. Must be SSL enabled. 2. Outbound NNTPS requests are proxied through the firewall to external servers. 3. Usage restricted by server-to-server source and destination IP.	1. A filter may be integrated to prevent accessing of objectionable newsgroups or content
20.	NTP	123	UDP	Denied	Cond.	Denied	1. For Navy NOCs only. 2. Version 3 or greater. 3. Source/Destination IP filtering required. 4. US Naval Observatory “navy.mil” time source required.	1. As NOCs are the only authorized users of this service across the Navy boundary, internal users will synch with the internal timing source provided by the NOC.
21.	Oracle SQLNET	1521, 1526	TCP	Cond.	Cond.	1. Requires ORACLE 8.x or greater. 2. Requires an ORACLE application proxy at the firewall if available. 3. Oracle Names Server use is not permitted.	1. Requires ORACLE 8.x or greater. 2. Requires an ORACLE application proxy at the firewall if available. 3. Oracle Names Server use is not permitted. 4. Destination IP filtering required.	1. As of 1 Jun 2004, only Oracle 8.1.6 is FIPS compliant. FIPS compliant version is required for use with Sensitive Information. 2. An alternative to port 1521/firewall proxy is to use ORACLE 8i with the Advanced Security Option for SSL encapsulation.

No.	Service	Port	Protocol	Policy		Conditions		Comments
				In	Out	In	Out	
22.	Oracle SQLNET - Navy – DoD Only	1601	TCP	Denied	Cond.	Denied	1. Only for use between Navy and DoD systems. Intra Navy systems must use ports 1521, 1526 as conditionally allowed in proceeding entry titled “Oracle SQLNET”. 2. Requires ORACLE 8.x or greater. 3. Requires an ORACLE application proxy at the firewall if available. 4. Oracle Names Server use is not permitted. 5. Destination IP filtering required.	1. As of 1 Jun 2004, only Oracle 8.1.6 is FIPS compliant. FIPS compliant version is required for use with Sensitive Information.
23.	OSPF		IP89	Cond.	Cond.	1. Fleet NOC use only.	1. Fleet NOC use only.	1. OSPF is allowed for Fleet NOC use only. 2. Due to movement of ships, limited dynamic routing is required through the firewall. This is accomplished by redistributing OSPF information through external BGP to external systems. Inbound routing information will not be allowed. The bastion host will run the gated daemon minimized for OSPF only and augmented with MD5 authentication to the inner and outer routers.

No.	Service	Port	Protocol	Policy		Conditions		Comments
				In	Out	In	Out	
24.	PPTP	1723	TCP, IP47	Denied	Denied	Denied	Denied	**NOTE: SPECIAL CASE: PPTP is permitted for DEERS/ RAPIDS use only. Section 4.2.1.3 germane.
25.	SMTP	25	TCP	Cond.	Cond.	1. Both inbound and outbound mail will be processed by a firewall proxy or equivalent. 2. Malicious code scanner required.	1. Both inbound and outbound mail will be processed by a firewall proxy or equivalent. 2. Outbound email will be allowed only from designated servers.	1. Anti-spam technology should be applied to the extent possible.
26.	SSH	22	TCP	Cond.	Cond.	1. Permitted only on a case-by-case basis by local Trusted Network DAA. 2. Must use SSH Protocol 2 or greater. 3. Allowed for Secure FTP and TELNET services only. Disable forwarding and tunneling. 4. Strong 2-factor authentication required. 5. Encryption must use FIPS-compliant algorithms for Sensitive Information.	1. Must use SSH Protocol 2 or greater. 2. Allowed for Secure FTP and TELNET services only. Disable forwarding and tunneling.	

No.	Service	Port	Protocol	Policy		Conditions		Comments
				In	Out	In	Out	
27.	SSL Encapsulated Proprietary Protocols	9000	TCP	Cond.	Cond.	1. Only to servers with DoD PKI server certs from authenticated users. 2. Minimum authentication requirement is utilization of SSL's inherent user ID and password capability. When available, client authentication must be done using DoD PKI certificates. 3. Must use IP filtering to host IP address. 4. Encryption must use FIPS-compliant algorithms for Sensitive Information.	1. Only to servers with DoD PKI server certs from authenticated users.	
28.	X.400	102	TCP	Cond.	Cond.	1. This service is restricted to DMS server-to-server source and destination routable address. 2. Inbound: Allowed only to authorized DMS servers.	1. This service is restricted to DMS server-to-server source and destination routable address. 2. Outbound: NAT off.	
29.	X.500	104, 17003	TCP	Cond.	Cond.	1. This service is restricted to DMS server-to-server source and destination routable address. 2. Allowed only to authorized DMS servers.	1. This service is restricted to DMS server-to-server source and destination routable address. 2. NAT off. 3. Proxy required.	1. This service is restricted to DMS source and destination address.
30.	X.500 SSL	105, 17004	TCP	Cond.	Cond.	1. This service is restricted to DMS source and destination address. 2. Proxy required. 3. Port use must include SSL and DoD PKI certificates.	1. This service is restricted to DMS source and destination address. 2. Proxy required. 3. Port use must include SSL and DoD PKI certificates.	1. Service restricted to use by DMS sites migrating from X.500 to X.500 SSL.

APPENDIX C. POSSIBLE VULNERABILITIES

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Adobe	Acrobat	Various PDF viewers including Adobe Acrobat 5.06 and Xpdf 1.01 allow remote attackers to execute arbitrary commands via shell meta characters in an embedded hyperlink.	High	Medium	Medium
Apache	Web Server	Apache 1.3 before 1.3.30, when running big-endian 64-bit platforms, does not properly parse Allow/Deny rules using IP addresses without a netmask, which could allow remote attackers to bypass intended access restrictions.	High	Low	Low
Apache	Web Server	The mod_alias and mod_rewrite modules of Apache fail to perform adequate boundary condition checking. A configuration file containing a regular expression of 9 capturing parentheses will trigger a buffer overflow allowing arbitrary data to be written to memory and executed. Local attackers able to create specially crafted files on the host can execute arbitrary commands on the targeted host. This problem was detected by matching the Apache banner to the list of affected Apache versions.	High	High	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Apache	Web Server	Cross-site scripting (XSS) vulnerability in Apache allows remote attackers to execute arbitrary web script and steal cookies via a URL with encoded newlines followed by a request to a .jsp file whose name contains the script.	Medium	High	Low
Apache	Web Server	mod_digest for Apache does not properly verify the nonce of a client response by using a AuthNonce secret.	Medium	Low	Low
Apache	Web Server	The mod_SSL add on module for the Apache Web server provides Secure Sockets Layer functionality. A buffer used by the ssl_compat_directive() function of mod_SSL is vulnerable to overflow when processing .htaccess files. This type of file is designed to provide access control policies for Web site users, and can be user defined if the "AllowOverride" Apache configuration variable has been set. The overflow can be triggered by setting the DATE_LOCALE variable to 10000 or more bytes. The excess data will be written to memory and processed by the host. Remote attackers can craft special .htaccess files, allowing them to execute arbitrary commands on targeted hosts.	High	Low	Medium

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
BSD	FreeBSD	The jail_attach system call in FreeBSD 5.1 and 5.2 changes the directory of a calling process even if the process doesn't have permission to change directory, which allows local users to gain read/write privileges to files and directories within another jail.	High	Medium	High
BSD	FreeBSD OpenBSD	Off-by-one error in the fb_realpath() function, as derived from the realpath function in BSD, may allow attackers to execute arbitrary code, as demonstrated in wu-ftpd 2.5.0 through 2.6.2 via commands that cause pathnames of length MAXPATHLEN+1 to trigger a buffer overflow, including (1) STOR, (2) RETR, (3) APPE, (4) DELE, (5) MKD, (6) RMD, (7) STOU, or (8) RNTO.	High	Low	High
BSD	FreeBSD NetBSD OpenBSD	The shmat system call in the System V Shared Memory interface for FreeBSD 5.2 and earlier, NetBSD 1.3 and earlier, and OpenBSD 2.6 and earlier, does not properly decrement a shared memory segment's reference count when the vm_map_find function fails, which could allow local users to gain read or write access to a portion of kernel memory and gain privileges.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
BSD	OpenBSD	OpenBSD kernel 3.3 and 3.4 allows local users to cause a denial of service (kernel panic) and possibly execute arbitrary code in 3.4 via a program with an invalid header that is not properly handled by (1) ibcs2_exec.c in the iBCS2 emulation (compat_ibcs2) or (2) exec_elf.c, which leads to a stack-based buffer overflow.	Medium	Low	Medium
BSD	XFree86	Multiple unknown vulnerabilities in XFree86 4.1.0 to 4.3.0, related to improper handling of font files.	Medium	Medium	Medium
BSD	XFree86	Buffer overflow in the ReadFontAlias function in XFree86 4.1.0 to 4.3.0, when using the CopyISOLatin1Lowered function, allows local or remote authenticated users to execute arbitrary code via a malformed entry in the font alias (font.alias) file.	High	Low	Medium
BSD	XFree86	Buffer overflow in ReadFontAlias from dirfile.c of XFree86 4.1.0 through 4.3.0 allows local users and remote attackers to execute arbitrary code via a font alias file (font.alias) with a long token.	High	Low	Medium

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
BSD	XFree86	Multiple integer overflows in the font libraries for XFree86 4.3.0 allow local or remote attackers to cause a denial of service or execute arbitrary code via heap-based and stack-based buffer overflow attacks.	High	Low	Medium
Cisco	Common Mngmt Foundation	CiscoWorks Common Management Foundation (CMF) 2.1 and earlier allows the guest user to gain administrative privileges via a certain POST request to com.cisco.nm.cmf.servlet. CsAuthServlet, possibly involving the "cmd" parameter with a modifyUser value and a modified "privileges" parameter.	High	Low	High
Cisco	Common Mngmt Foundation	CiscoWorks Common Management Foundation (CMF) 2.1 and earlier allows the guest user to obtain restricted information and possibly gain administrative privileges by changing the "guest" user to the Admin user on the Modify or delete users pages.	High	High	High
Cisco	IOS	Buffer overflow in the HTTP server for Cisco IOS 12.2 and earlier allows remote attackers to execute arbitrary code via an extremely long (2GB) HTTP GET request. This allows an attacker to be able to execute commands to view and modify configuration data.	High	High	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Cisco	IOS	Multiple vulnerabilities in the H.323 protocol implementation for Cisco IOS 11.3T through 12.2T allow remote attackers to cause a denial of service and possibly execute arbitrary code, as demonstrated by the NISCC/OUSPG PROTOS test suite for the H.225 protocol.	High	Low	Medium
Cisco	Personal Assistant	Cisco Personal Assistant 1.4(1) and 1.4(2) disables password authentication when “Allow Only Cisco CallManager Users” is enabled and the Corporate Directory settings refer to the directory service being used by Cisco CallManager, which allows remote attackers to gain access with a valid username.	High	High	High
IBM	DB2	Stack-based buffer overflow in IBM DB2 Universal Data Base 7.2 before Fixpak 10 and 10a, and 8.1 before Fixpak 2, allows attackers with “Connect” privileges to execute arbitrary code via a LOAD command.	High	Low	Medium
Linksys	EtherFast Router	VPN Server module in Linksys EtherFast BEFVP41 Router before 1.40.1 reduces the key lengths for keys that are supplied via manual key entry, which makes it easier for attackers to crack the keys.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Linksys	WAP11	SNMP service in Atmel 802.11b VNET-B Access Point 1.3 and earlier, as used in Netgear ME102 and Linksys WAP11, accepts arbitrary community strings with requested MIB modifications, which allows remote attackers to obtain sensitive information such as WEP keys, cause a denial of service, or gain access to the network.	High	High	High
Microsoft	Access 2003	Buffer overflow in the ActiveX control for Microsoft Access Snapshot Viewer for Access 2003 allows remote attackers to execute arbitrary code via long parameters to the control.	High	High	High
Microsoft	ASP.Net	Microsoft ASP.Net 1.1 allows remote attackers to bypass the Cross-Site Scripting (XSS) and Script Injection protection feature via a null character in the beginning of a tag name.	High	Low	Low
Microsoft	Excel 2003	Microsoft Excel 2003 allows remote attackers to execute arbitrary code via a spreadsheet with a malicious XLM (Excel 4) macro that bypasses the macro security model.	Low	Medium	Low

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Exchange Server	Cross-site scripting (XSS) vulnerability in the HTML encoding for the Compose New Message form in Microsoft Exchange Server 5.5 Outlook Web Access (OWA) allows remote attackers to execute arbitrary web script.	Medium	Medium	Medium
Microsof t	Exchange Server Exchange 2000	The Internet Mail Service in Exchange Server 5.5 and Exchange 2000 allows remote attackers to cause a denial of service (memory exhaustion) by directly connecting to the SMTP service and sending a certain extended verb request, possibly triggering a buffer overflow in Exchange 2000.	Medium	Medium	Medium
Microsof t	FrontPage	Buffer overflow in the debug functionality in fp30reg.dll of Microsoft FrontPage Server Extensions 2000 and 2002 allows remote attackers to execute arbitrary code via a certain chunked encoded request.	Low	High	Low
Microsof t	Internet Explorer	Internet Explorer 6 SP1 allows remote attackers to direct drag and drop behaviors and other mouse click actions to other windows by using method caching (SaveRef) to access the window.moveBy method, which is otherwise inaccessible, a.k.a. “Hijack Click V.2”.	Low	Low	Low

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Internet Explorer	Microsoft Internet Explorer allows remote attackers to bypass intended cookie access restrictions on a web application via “%2e%2e” (encoded dot dot) directory traversal sequences in a URL, which causes Internet Explorer to send the cookie outside the specified URL subsets, e.g. to a vulnerable application that runs on the same server as the target application.	Low	Low	Low
Microsof t	Internet Explorer	Internet Explorer 6 SP1 and earlier allows remote attackers to direct drag and drop behaviors and other mouse click actions to other windows by calling the window.moveBy method, a.k.a. Hijack Click.	Low	Low	Low
Microsof t	Internet Explorer	Internet Explorer allows remote attackers to bypass zone restrictions to inject and execute arbitrary programs by creating a popup window and inserting ActiveX object code with a “data” tag pointing to the malicious code, which Internet Explorer treats as HTML or Javascript, but later executes as an HTA application, as exploited using the QHosts Trojan horse (a.k.a. Trojan.Qhosts, QHosts-1, VBS.QHOSTS, or aolfix.exe).	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsoft	Internet Explorer	Internet Explorer 6 SP1 and earlier allows remote attackers to bypass zone restrictions by (1) using the NavigateAndFind method to load a file: URL containing Javascript, as demonstrated by NAFfileJPU, (2) using the window.open method to load a file: URL containing Javascript, as demonstrated using WsOpenFileJPU, (3) setting the href property in the base tag for the _search window, as demonstrated using WsBASEjpu, (4) loading the search window into an Iframe, as demonstrated using WsFakeSrc, (5) caching a javascript: URL in the browser history, then accessing that URL in the same frame as the target domain, as demonstrated using WsOpenJpuInHistory, NAFjpuInHistory, BackMyParent, BackMyParent2, and RefBack, a.k.a. the "Script URLs Cross Domain" vulnerability.	Low	Low	Low
Microsoft	Internet Explorer	Internet Explorer 5.01 through 6 SP1 allows remote attackers to bypass zone restrictions and read arbitrary files via an XML object.	Low	Low	Low

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsoft	Internet Explorer	Internet Explorer 6 SP1 and earlier allows remote attackers to bypass zone restrictions and execute Javascript by setting the window's "href" to the malicious Javascript, then calling execCommand("Refresh") to refresh the page, aka BodyRefreshLoadsJPU or the "ExecCommand Cross Domain" vulnerability.	Low	Low	Low
Microsoft	Internet Explorer	Internet Explorer 6 SP1 allows remote attackers to bypass zone restrictions via a javascript protocol URL in a sub-frame, which is added to the history list and executed in the parent's top window's zone when the history.back (back) function is called, as demonstrated by BackToFramedJpu.	Low	Low	Low
Microsoft	Internet Explorer	Internet Explorer 6, and possibly other versions, allows remote attackers to spoof the domain of a URL via a "%01" character before an @ sign in the user@domain portion of the URL, which hides the rest of the URL, including the real site, in the address bar.	Medium	Medium	Medium

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Internet Explorer	Internet Explorer 5.01 through 6.0 does not properly handle object tags returned from a Web server during XML data binding, which allows remote attackers to execute arbitrary code via an HTML e-mail message or web page.	High	Medium	High
Microsof t	Internet Explorer	Buffer overflow in Internet Explorer 6 SP1 for certain languages that support double-byte encodings (e.g., Japanese) allows remote attackers to execute arbitrary code via the Type property of an Object tag.	High	Medium	High
Microsof t	Internet Explorer	Buffer overflow in the BR549.DLL ActiveX control for Internet Explorer 5.01 SP3 through 6.0 SP1 allows remote attackers to execute arbitrary code.	High	Low	High
Microsof t	Internet Explorer	Internet Explorer 5.01 SP3 through 6.0 SP1 does not properly determine object types that are returned by web servers, which could allow remote attackers to execute arbitrary code via an object tag with a data parameter to a malicious file hosted on a server that returns an unsafe Content-Type, a.k.a. the "Object Type" vulnerability.	High	Medium	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Internet Explorer	Internet Explorer 6 SP1 and earlier allows remote attackers to bypass zone restrictions and read arbitrary files by (1) modifying the createTextRange method and using CreateLink, as demonstrated using LinkillerSaveRef, LinkillerJPU, and Linkiller, or (2) modifying the createRange method and using the FIND dialog to select text, as demonstrated using Findeath, a.k.a. the “Function Pointer Override Cross Domain” vulnerability.	High	Medium	High
Microsof t	Message Queue Manager	Buffer overflow in the Microsoft Message Queue Manager (MSQM) allows remote attackers to cause a denial of service (RPC service crash) via a queue registration request.	High	Low	High
Microsof t	Outlook Express	The MHTML protocol handler in Microsoft Outlook Express 5.5 SP2 through Outlook Express 6 SP1 allows remote attackers to bypass domain restrictions and execute arbitrary code, as demonstrated on Internet Explorer using script in a compiled help (CHM) file that references the InfoTech Storage (ITS) protocol handlers such as (1) ms-its, (2) ms-itss, (3) its, or (4) mk:@MSITStore, a.k.a. the “MHTML URL Processing Vulnerability.”	Medium	Low	Low

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Outlook Express	Microsoft Outlook Express does not sufficiently filter parameters of mailto: URLs when using them as arguments when calling OUTLOOK.EXE, which allows remote attackers to use script code in the Local Machine zone and execute arbitrary programs.	High	Medium	High
Microsof t	SQL Server	Microsoft SQL Server before Windows 2000 SP4 allows local users to gain privileges as the SQL Server user by calling the xp_fileexist extended stored procedure with a named pipe as an argument instead of a normal file.	High	Low	High
Microsof t	SQL Server	Microsoft SQL server is a enterprise level database. Often due to SQL database installation complexity, many users use the default system administrator username with no password for authentication. This error can lead to a remote attacker controlling your entire database including any customer information such as credit card numbers, home phones, addresses, etc.	High	High	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	SQL Server MSDE	SQL Server and MSDE fail to properly validate requests on certain LPC ports. A specially formed packet sent to an LPC port can overflow an allocated buffer. Data outside the buffer range will be placed into memory and executed. A local attacker with limited access can escalate their privileges on targeted hosts by triggering the overflow to execute code within the security context of the SQL Server account.	High	Low	High
Microsof t	SQL Server MSDE	A flaw in the authentication methods used by SQL Server and MSDE allow a named pipe session to be hijacked. Once a local attacker has gained control of the named pipe they can then execute the same commands as the client authenticating through that specific named pipe. If access privileges are higher, arbitrary SQL commands can be executed.	High	High	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Visual Basic	Visual Basic for Applications (VBA), which is used to run scripts in Microsoft Office applications, fails to perform adequate boundary condition checking when opening documents and allows an allocated buffer to be overrun. Data outside of the buffer will be written to memory and executed. Remote attackers can create malicious Office documents to trigger the overflow and execute arbitrary code on targeted hosts. A user would have to open the document for the code to be executed.	High	Low	High
Microsof t	Windows 2000	The Utility Manager in Microsoft Windows 2000 executes winhlp32.exe with system privileges, which allows local users to execute arbitrary code via a “Shatter” style attack using Windows messages, as demonstrated using the File Open dialog in the Help window.	High	Medium	High
Microsof t	Windows 2000	A buffer overflow in Troubleshooter ActiveX Control (Tshoot.ocx) in Microsoft Windows 2000, SP4 and earlier allows remote attackers to execute arbitrary code via an HTML formatter e-mail or web page.	High	Medium	Medium

Vendor	**Software/ Hardware**	**Vulnerability Description**	**Magnitude of Impact**	**Likelihood of Successful Exploitation**	**Assigned Level of Risk**
Microsof t	Windows XP	Windows XP allows local users to execute arbitrary programs by creating a task at an elevated privilege level through the eventtriggers.exe command-line tool or the Task Scheduler service, a.k.a. “Windows Management Vulnerability.”	High	High	High
Microsof t	Windows NT 4.0 Windows 2000	The component for the Virtual DOS Machine (VDM) subsystem in Windows NT 4.0 and Windows 2000 does not properly validate system structures, which allows local users to access protected kernel memory and execute arbitrary code.	High	Low	Medium
Microsof t	Windows NT 4.0 Windows 2000	The NtSetLdtEntries function in the programming interface for the Local Descriptor Table (LDT) in Windows NT 4.0 and Windows 2000 allows local attackers to gain access to kernel memory and execute arbitrary code via an expand-down data segment descriptor that points to protected memory.	High	Low	Medium
Microsof t	Windows NT 4.0 Windows Server 2003	The Windows Internet Naming Service (WINS) for Microsoft Windows Server 2003, and possibly Windows NT, does not properly validate the length of certain packets, which allows attackers to cause a denial of service and possibly execute arbitrary code.	High	High	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Windows XP Windows Server 2003	Help and Support Center in Microsoft Windows XP and Windows Server 2003 SP1 does not properly validate HCP URLs, which allows remote attackers to execute arbitrary code, as demonstrated using certain hcp:// URLs that access the DVD Upgrade capability (dvdupgrd.htm).	High	High	High
Microsof t	Windows XP Windows Server 2003	Stack-based buffer overflow in the PCHealth system in the Help and Support Center function in Windows XP and Windows Server 2003 allows remote attackers to execute arbitrary code via a long query in an HCP URL.	High	High	High
Microsof t	Windows 2000 Windows XP Windows Server 2003	Unknown vulnerability in the H.323 protocol implementation in Windows 2000, Windows XP, and Windows Server 2003 allows remote attackers to execute arbitrary code.	High	Medium	Medium
Microsof t	Windows 2000 Windows XP Windows Server 2003	The Negotiate Security Software Provider (SSP) interface in Windows 2000, Windows XP, and Windows Server 2003, allows remote attackers to cause a denial of service (crash from null dereference) or execute arbitrary code via a crafted SPNEGO NegTokenInit request during authentication protocol selection.	High	Medium	Medium

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Windows NT 4.0 Windows 2000 Windows XP	Multiple integer overflows in Microsoft ASN.1 library (MSASN1.DLL), as used in LSASS.EXE, CRYPT32.DLL, and other Microsoft executables and libraries on Windows NT 4.0, 2000, and XP, allow remote attackers to execute arbitrary code via ASN.1 BER encodings with very large length fields that cause arbitrary heap data to be overwritten.	High	Low	High
Microsof t	Windows NT 4.0 Windows 2000 Windows XP	Buffer overflow in the rendering for (1) Windows Metafile (WMF) or (2) Enhanced Metafile (EMF) image formats in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, and XP SP1allows remote attackers to execute arbitrary code via a malformed WNF or EMF image.	High	Low	High
Microsof t	Windows NT 4.0 Windows 2000 Windows XP	A multi-threaded race condition in the Windows RPC DCOM functionality with the MS03-039 patch installed allows remote attackers to cause a denial of service (crash or reboot) by causing two threads to process the same RPC request, which causes one thread to use memory after it has been freed, as demonstrated by certain exploits against those vulnerabilities.	High	Medium	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Windows NT 4.0 Windows 2000 Windows XP	Buffer overflow in the SMB capability for Microsoft Windows XP, 2000, and NT allows remote attackers to cause a denial of service and possibly execute arbitrary code via an SMB packet that specifies a smaller buffer length than is required.	High	Low	High
Microsof t	Windows NT 4.0 Windows 2000 Windows XP Windows Server 2003	Stack-based buffer overflow in a logging function for Windows Workstation Service (WKSSVC.DLL) allows remote attackers to execute arbitrary code via RPC calls that cause long entries to be written to a debug log file (“NetSetup.LOG”), as demonstrated using the NetAddAlternateComputerName API.	High	Low	High
Microsof t	Windows NT 4.0 Windows 2000 Windows XP Windows Server 2003	Microsoft Data Access Components (MDAC) provide connectivity between Windows clients and various different data source types. The MDAC components have an unchecked buffer in the function that handles replies to SQL broadcast requests. The buffer overflow allows attackers to execute arbitrary code on systems that create SQL broadcast requests to discover SQL servers. Attackers can exploit this vulnerability by hosting a malicious SQL server that responds with malformed SQL/MDAC responses to the requesting machine.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Windows NT 4.0 Windows 2000 Windows XP Windows Server 2003	The Microsoft ASN.1 library is used to pass messages in a variety of protocols such as SNMP and NTLMv2. A malformed ASN.1 message can lead to the exploitation of a remote code execution flaw on a variety of Microsoft platforms.	High	Medium	High
Microsof t	Windows NT 4.0 Windows 2000 Windows XP Windows Server 2003	Two DirectX functions used to process MIDI audio files do not perform proper bounds checking and are vulnerable to buffer overflow atttacks. Remote attackers can craft a malicious MIDI file to distribute from a Web server they control. A user who views this file from one of the affected applications will then execute the malicious content of the file. Execution occurs in the context of the user viewing the file. Successful exploitation of this vulnerability requires that a user download and execute the malicious media file.	High	Low	Medium
Microsof t	Windows NT 4.0 Windows 2000 Windows XP Windows Server 2003	Multiple integer overflows in a Microsoft Windows DirectX MIDI library (QUARTZ.DLL) allow remote attackers to execute arbitrary code via a MIDI (.mid) file with (1) large length for a Text or Copyright string, or (2) a large number of tracks, which leads to a heap-based buffer overflow.	High	Low	Medium

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Windows NT 4.0 Windows 2000 Windows XP Windows Server 2003	The HTML encoder provided by the copy-paste functionality within Microsoft Windows contains an exploitable buffer overrun. A buffer overflow in the HTML encoder can be exploited to allow an attacker to execute arbitrary code. This vulnerability can be exploited by an attacker who hosts a malicious web site that the user views or via a malicious HTML-based email sent to the end-user.	High	Low	High
Microsof t	Windows NT 4.0 Windows 2000 Windows XP Windows Server 2003	The Distributed Component Objects Model (DCOM) protocol and Remote Procedure Call (RPC) service are installed with many Microsoft Windows operating systems. DCOM allows the distribution of application components across multiple servers. The RPC service listens on TCP port 135, and handles DCOM object requests sent to the server. The RPC service fails to adequately validate messages sent to the service, allowing a buffer to be overrun. Data outside of the buffer will be executed on the server with SYSTEM user privileges. Remote attackers can exploit this vulnerability to execute arbitrary commands on the targeted host.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Windows NT 4.0 Windows 2000 Windows XP Windows Server 2003	Buffer overflow in a certain DCOM interface for RPC in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 allows remote attackers to execute arbitrary code via a malformed message.	High	Low	High
Microsof t	Windows NT 4.0 Windows 2000 Windows XP Windows Server 2003	The Microsoft Windows Messenger Service transmits messages to network users and the Alerter Service for Windows. It is not related to the Windows or MSN Messenger instant messaging applications. The Messenger Service fails to validate the size of messages allowing an allocated buffer to be overflowed. Data outside the buffer will be placed in memory and processed with SYSTEM level privileges or cause the service to stop responding. Remote attackers can send specially crafted messages allowing them to execute arbitrary code on targeted hosts.	High	Low	High
Microsof t	Windows NT 4.0 Windows 2000 Windows XP Windows Server 2003	Heap-based buffer overflow in the Distributed Component Object Model (DCOM) interface in the RPCSS Service allows remote attackers to execute arbitrary code via a malformed DCERPC DCOM object activation request packet with modified length fields.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsoft	Windows NT 4.0 Windows 2000 Windows XP Windows Server 2003	Buffer overflow in a certain component of Microsoft Data Access Components (MDAC) 2.5 through 2.7 allows remote attackers to execute arbitrary code via a certain response to a broadcast address.	High	Low	High
Microsoft	Window NT 4.0 Windows 2000 Windows XP Windows Server 2003	The Authenticode capability in Microsoft, Windows NT, through Server 2003 does not prompt the user to download and install ActiveX controls when the system is low on memory, which could allow remote attackers execute arbitrary code without user approval.	High	High	High
Microsoft	Window NT 4.0 Windows 2000 Windows XP Windows Server 2003	Buffer overflow in a function in User32.dll on Windows NT through Server 2003 allows local users to execute arbitrary code via long (1) LB_DIR messages to ListBox or (2) CB_DIR messages to ComboBox controls in a privileged application.	High	Low	High
Microsoft	Windows NT 4.0 Windows 2000 Windows XP Windows Server 2003	Buffer overflow in the streaming media component for logging multicast requests in the ISAPI for the logging capability of Microsoft Windows Media Services (nsiislog.dll), as installed in IIS 5.0, allows remote attackers to execute arbitrary code via a large POST request to nsiislog.dll.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Microsof t	Word 2003	Microsoft Word 2000 does not properly check certain properties of a document, which allows attackers to bypass the macro security model and automatically execute arbitrary macros via a malicious document.	High	High	High
Microsof t	Word 2003 Works Suite	Microsoft Word 2003, and Microsoft Works Suites 2001 through 2004 do not properly check the length of the “Macro names” data value, which could allow remote attackers to execute arbitrary code via a buffer overflow attack.	High	High	High
Norton	Antivirus Antivirus Pro	The GUI functionality for an interactive session in Symantec LiveUpdate 1.70.x through 1.90.x, as used in Norton Internet Security 2001 through 2004, SystemWorks 2001 through 2004, and AntiVirus and Norton AntiVirus Pro 2001 through 2004, AntiVirus for Handhelds v3.0, allows local users to gain SYSTEM privileges.	High	Medium	Medium
Open Source	Ghostscript	Unknown vulnerability in GNU Ghostscript before 7.07 allows attackers to execute arbitrary commands, even when -dSAFER is enabled, via a malicious PostScript file.	High	Low	Medium

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Open Source	Konqueror	Konqueror Embedded and KDE 2.2.2 and earlier does not validate the Common Name (CN) field for X.509 Certificates, which could allow remote attackers to spoof certificates via a man-in-the-middle attack.	High	High	High
Open Source	Konqueror	Buffer overflow in KON kon2 0.3.9b and earlier allows local users to execute arbitrary code via a long -Coding command line argument.	High	Low	High
Open Source	Linux	Integer overflow in the ip_setsockopt function in Linux kernel 2.4.22 through 2.4.25 and 2.6.1 through 2.6.3 allows local users to cause a denial of service (crash) or executee arbitrary code via the MCAST_MSFILTER socket option.	High	Low	High
Open Source	Linux	The mremap system call (do_mremap) in Linux kernel 2.2, 2.4, and 2.6 does not properly perform bounds checks, which allows local users to cause a denial of service and possibly gain privileges by causing a remapping of a virtual memory area (VMA) to create a zero length VMA.	High	Medium	High
Open Source	Linux	Buffer overflow in the HTTP parser for MPlayer 1.0pre3 and earlier, 0.90, and 0.91 allows remote attackers to execute arbitrary code via a long Location header.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Open Source	Linux	The do_mremap function for the mremap in Linux 2.2 to 2.2.25, 2.4 to 2.4.24, and 2.6 to 2.6.2, does not properly check the return value from the do_munmap function when the maximum number of VMA descriptors is exceeded, which allows local users to gain root privileges.	High	Low	High
Open Source	Linux	Multiple buffer overflows in vfte, based on fte, before 0.50, allow local users to execute arbitrary code.	High	Low	High
Open Source	Linux	Heap-based buffer overflow in rsync before 2.5.7, when running in server mode, allows remote attackers to execute arbitrary code and possibly escape the chroot jail.	High	Low	High
Open Source	Linux	Multiple buffer overflows in (1) iso2022jp.c or (2) shiftjis.c for Courier-IMAP before 3.0.0, Courier before 0.45, and SqWebMail before 4.0.0 may allow remote attackers to execute arbitrary code “when Unicode character is out of BMP range.”	High	Low	High
Open Source	Linux	Format string vulnerability in LinuxNode (node) before 0.3.2 may allow attackers to cause a denial of service or execute arbitrary code.	High	High	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Open Source	Linux	Buffer overflow in LinuxNode (node) before 0.3.2 allows remote attackers to execute arbitrary code.	High	Low	High
Open Source	Linux	Unknown vulnerability in the ncp_lookup function of ncpfs in Linux 2.1 allows local users to gain privileges.	High	Low	Medium
Open Source	Linux	A “flaw in bounds checking” in the do_brk function for Linux kernel 2.4.22 and earlier allows local users to gain root privileges.	High	Low	High
Open Source	Linux	The getgrouplist function in GNU libc allows may attackers to cause a denial of service (segmentation fault) and execute arbitrary code when a user is a member of a large number of groups, which can cause a buffer overflow.	High	High	High
Open Source	Linux	The RPC code in Linux kernel 2.4 sets the reuse flag when sockets are created, which could allow local users to bind to UDP ports that are used by privileged services such as nfsd.	High	Medium	Medium
Open Source	Linux	The mxcsr code in Linux kernel 2.4 allows attackers to modify CPU state registers via a malformed address.	High	Medium	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Open Source	Linux	The Linux 2.0 kernel IP stack does not properly calculate the size of an ICMP citation, which causes it to include portions of unauthorized memory in ICMP error responses.	High	Low	Medium
Open Source	Metamail	Multiple buffer overflows in Metamail 2.7 and earlier allow remote attackers to execute arbitrary code.	High	Low	High
Open Source	Metamail	Multiple format string vulnerabilities in Metamail 2.7 and earlier allow remote attackers to execute arbitrary code.	High	Medium	Medium
Open Source	MySQL	When installed, MySQL enables world-writeable files. Using the OUTFILE SQL command, attackers can overwrite configuration files and cause the MySQL daemon to start with elevated privileges. This allows remote attackers to execute arbitrary actions on the targeted host.	High	High	High
Open Source	MySQL	Buffer overflow in get_salt_from_password from sql_acl.cc for MySQL 4.0.14 and earlier, and 3.23.x, allows attackers to execute arbitrary code via a long Password field	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Open Source	MySQL	MySQL allows authorized users to switch to a different user account using the COM_CHANGE_USER command. Inadequate bounds checking allows any password greater than 16 characters that is parsed by COM_CHANGE_USER to cause a buffer overflow condition. Arbitrary data outside the buffer may be executed with elevated privileged or cause the MySQL daemon (mysqld) to crash. This allows attackers with access to a valid account to cause a denial-of-service condition or run arbitrary code on the targeted host.	High	Low	High
Open Source	Opera	Opera allows remote attackers to bypass intended cookie access restrictions on a web application via “%2e%2e” (encoded dot dot) directory traversal sequences in a URL, which causes Opera to send the cookie outside the specified URL subsets, e.g. to a vulnerable application that runs on the same server as the target application.	High	Medium	Medium

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Open Source	Samba	Samba is an open source software suite that provides file and print services through Server Message Block/Common Internet File Sharing (SMB/CIFS) for UNIX and Windows systems. It packaged with most Linux distributions. A portion of the Samba source code contains insecure coding methods that allow a buffer to be exceeded. The issue lies within the call_trans2open function in trans2.c that allocates a buffer of 1024 bytes. It is possible to write data outside the buffer, which is then placed on the process stack. This allows remote attackers to run arbitrary commands on the targeted host by embedding them in specially crafted requests to the intended victim.	High	Low	High
Open Source	tcpdump	tcpdump before 3.8.1 allows remote attackers to cause a denial of service (infinite loop) via certain ISAKMP packets.	High	Medium	Medium

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Open Source	Wu-ftpd	The Washington University (WU) FTP server package improperly processes user input in such a way as to allow for a remote attacker to overwrite one word in memory with arbitrary data. It is possible to exploit this vulnerability in order to gain root privileges on the target system. This attack requires an attacker to login to the FTP server with any valid user account including the anonymous user account prior to exploitation. Affected versions of this package include WU-FTPD 2.5.0, 2.6.0 and 2.6.1. No public exploit exists for this vulnerability however private exploits are believed to exist.	High	Low	High
Sun	AnswerBook	Some versions of Solaris include the Sun AnswerBook2 Documentation Server. It provides network access to the documentation for Sun products. The 'gettransbitmap' CGI component of AnswerBook2 does not perform adequate boundary condition checking. Passing a long filename argument to the gettransbitmap CGI will cause an overrun buffer, allowing an attacker to execute commands on the targeted host.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Sun	KCMS	The Kodak Color Management System (KCMS) Library is a color management API for Sun Solaris. The KCMS daemon allows remote clients to access color profiles stored on the host. The daemon parses directory traversal commands in KCS_OPEN_PROFILE requests allowing access to files outside of the /usr/openwin/etc/devdata/profiles or /etc/openwin/devdata/profiles directories. Remote attackers can access arbitrary files on the host be specifying the absolute path in the fileName argument. This includes allowing access to /etc/shaddow or /etc/passwd with account usernames and passwords.	High	Low	Medium
Sun	Solaris	Unknown vulnerability in the ls-F builtin function in tcsh on Solaris 8 allows local users to create or delete files as other users, and gain privileges.	High	High	High
Sun	Solaris	Unknown multiple vulnerabilities in (1) lpstat and (2) the libprint library in Solaris 2.6 through 9 may allow attackers to execute arbitrary code or read or write arbitrary files.	High	Medium	Medium

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Sun	Solaris	In Sun Solaris, it is possible to identify and crash the RPC snmpXdmi daemon. This daemon is vulnerable to a remote buffer overflow that may be exploited to gain remote root control of the target system.	High	Low	High
Sun	Solaris	The ypbind daemon fails to perform adequate boundary condition checking, allowing buffer overflows to occur. Data outside of the buffer range is placed in memory and executed by the host with root privileges; or it can cause the daemon to crash. Remote attackers can execute arbitrary commands on target hosts by sending specially-crafted requests to the ypbind service over TCP port 111. If the ypbind daemon crashes as a result of an overflow, subsequent NIS lookups will fail resulting in a denial-of-service condition.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Sun	Solaris	The Calendar Manager RPC daemon is a small database manager for appointment and resource scheduling data. The daemon fails to perform adequate boundary condition checks, permitting a buffer overflow to occur. Remote attackers can exploit the buffer overflow to execute arbitrary instructions and gain root access on targeted hosts by sending specially-crafted requests to the daemon.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Sun	Solaris	Remote Procedure Call (RPC) is a library for inter-process communication within a system. The xdr_array function is standard in all Sun RPC implementations. XDR primitives are routines that allow a uniform presentation of basic data types. The xdr_array filter primitive translates variable-length arrays. An attacker can pass a large number of elements to xdr_array, causing a buffer overflow condition. This allows an attacker to execute arbitrary commands on the targeted host with super-user privileges. Other RPC services on many UNIX platforms may be vulnerable because xdr_array is not specific to any one service. Any RPC service that uses xdr_array could be vulnerable. By default, RPC services are installed and enabled on the vulnerable software versions.	High	Low	High
Sun	Solaris	Abuffer overflow vulnerability exists within Sun Solaris snmpdx which may allow for an attacker gain complete control of the target host, and the snmpdx daemon is installed by default with the Sun Solaris operating system.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Sun	Solaris	The default installation of sadmind on Solaris uses weak authentication (AUTH_SYS), which allows local and remote attackers to spoof Solstice AdminSuite clients and gain root privileges via a certain sequence of RPC packets.	High	Medium	High
Sun	Solaris	Stack-based buffer overflow in the runtime linker, ld.so.1, on Solaris 2.6 through 9 allows local users to gain root privileges via a long LD_PRELOAD environment variable.	High	Low	High
Sun	Solaris	A buffer overflow vulnerability exists within many versions of the Unix system V based login program in how environment variables are processed. It is possible for an attacker to locally exploit a vulnerable login program or to connect to a telnet or rlogin daemon that uses a vulnerable login program and supply specially crafted data that allows for remote execution of arbitrary code on the target system.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Sun	Solaris	The cachefsd daemon is installed by default on all versions of Sun's Solaris operating systems. Cachefsd is used to cache requests for operations on remote file systems which are mounted using the NFS protocol. The problem is due to insufficient bounds checking on the mounts that were supplied by the user. An attacker may exploit this vulnerability by creating a file and having the cachefsd process it to gain root privileges.	High	Low	High
Sun	ToolTalk	The ToolTalk component allows applications to communicate via remote procedure calls (RPC) across different hosts and platforms. The ToolTalk RPC database is used to manage connections between ToolTalk applications. The _TT_CREATE_FILE procedure within the ToolTalk RPC database is vulnerable to a buffer overflow. An attacker may exploit this vulnerability in order to run attacker specified code with the privileges of the ToolTalk RPC database server. By default the ToolTalk server runs as root.	High	Low	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
SuSE	Linux Pro	SuSEconfig.susewm in the susewm package on SuSE Linux 8.2Pro allows local users to overwrite arbitrary files via a symlink attack on the susewm.$$ temporary file.	High	High	High
SuSE	Linux Pro	SuSEconfig.javarunt in the javarunt package on SuSE Linux 7.3Pro allows local users to overwrite arbitrary files via a symlink attack on the .java_wrapper temporary file.	High	High	High
Various	Telnet daemon	A vulnerability in many vendor-supplied Telnet daemons can be exploited by sending large amounts of data in telnet environment variables. By doing so, values on the heap are overwritten and program flow may be redirected.	High	Low	High
Various	X11	X11 is a client/server protocol. The server controls the screen and the clients connected to it. The client sends several requests like drawing a window or a menu and the server sends back to them events such as mouse clicks, key strokes. Many users have their X Server set to xhost +, permitting access to the X Server by anyone, from anywhere. This misconfiguration can lead to fairly quick compromise by sniffing the xterm keystrokes from root users.	High	High	High

Vendor	Software/ Hardware	Vulnerability Description	Magnitude of Impact	Likelihood of Successful Exploitation	Assigned Level of Risk
Various	SMTP	The parseaddr.c portion of Sendmail is responsible for parsing Email addresses in SMTP headers. The prescan() function in parseaddr.c fails to perform adequate bounds checking, and allows an associated buffer to be overflowed. A special control value in this function allows boundary condition checks to be bypassed. By crafting special SMTP requests remote attackers place arbitrary data on the process stack. This data will be executed or cause a denial-of-service condition on the targeted host.	High	Low	High
Various	SMTP	A “potential buffer overflow in ruleset parsing” for Sendmail 8.12.9, when using the nonstandard rulesets (1) recipient (2), final, or (3) mailer-specific envelope recipients, has unknown consequences.	High	Low	High
Various	SMTP	Inadequate boundary condition checks in Sendmail allow arbitrary data to processed by the Sendmail daemon. A HELO command in excess of 1024 characters will trigger the overflow, and allows remote attackers to execute arbitrary code on the targeted host. The popular use of this attack is to send SMTP traffic from the targeted host, thereby disguising the actual source.	High	Low	High

LIST OF REFERENCES

1. National Security Telecommunications and Information Systems Security Instruction 4009, National Information Systems Security Glossary, September 2000.

2. Working Group on California Earthquake Probabilities, “Earthquake Probabilities in the San Francisco Bay Region: 2000 to 2030 - A Summary of Findings,” 1999.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

DoD Instruction 5200.40, Department of Defense Information Technology Security Certification and Accreditation Process, December 1997.

DoD Directive 8500.1, Department of Defense Information Assurance, October 2002.

DoD Directive 8500.2, Department of Defense Information Assurance Implementation, February 2003.

Chief of Naval Operations Information Assurance Pub 5239-01, Introduction to Information Systems Security, May 2000.

Chief of Naval Operations Information Assurance Pub 5239-13 Volumes 1-3, Certification and Accreditation Publication, various dates.

Chief of Naval Operations Information Assurance Pub 5239-16, Risk Assessment Guidebook, March 2003.

Symantec, “Behind the Firwall: The Insider Threat,” http://www.symantec.com/symadvantage/017/insider.html, Winter 2003.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California